

KURUMSAL RİSK YÖNETİMİ: SORUMLULAR VE BAŞARI KRİTERLERİ ÜZERİNDEN BİR DEĞERLENDİRME

(ENTERPRISE RISK MANAGEMENT: AN ASSESSMENT ON
RESPONSIBILITIES AND SUCCESS CRITERIA PUBLIC ADMINISTRATION)

Mehmet Akif ÖZER * / Emrah ERDEM **

ÖZ

Risk yönetimi en genel şekliyle bir kuruluşun müşterilerini (vatandaş, özel sektör ve sivil toplum kuruluşları), personeli ve kendisini korumak için ileride karşılaşabileceği ve maruz kaldığı belirsizlik ve tehditlerin yönetilerek gelişim potansiyelinin artırılmasıdır. Kurumsal Risk Yönetimi (KRY) ise bu çalışmaların KRY çerçevesi esas alınarak kurum içinde sistemli hale getirilmesidir. Gerek İngilizcede gerekse Türkçede “risk” kayıp hasar derecesi ya da bunların olasılığı olarak tanımlanmıştır. Hem risk yönetimi hem de kurumsal risk yönetimi bu kavram üzerinden kuramlaştırılmıştır. Çalışmanın odağında yer alan Kurumsal Risk Yönetimi, bir kuruluşun hedeflerine ulaşmasını etkileyebilecek potansiyel olayları tanımlayan, risk alma istekliliği sınırları içinde yöneten ve kuruluş hedeflerinin başarılması konusunda makul derecede güvence sağlayan, kuruluş genelinde yapılandırılmış ve yönetim kurulundan, yönetimden

ve diğer çalışanlardan etkilenen bir süreçtir. Bu süreçte başarı kriterleri kapsamında en önemli unsurlar, başta üst düzey yöneticiler olmak üzere kuruluşun tüm çalışanlarıdır. Çalışmada Kurumsal Risk Yönetiminin etkinliğinin söz konusu bu sorumlulara bağlı olduğu varsayımından hareket edilmektedir. Bu doğrultuda önce risk ve risk yönetimi ile ilgili kavramsal çerçeve ortaya konacak ardından Kurumsal Risk Yönetimi ve son kısımda da söz konusu bu sistemin organizasyon yapısı ve sorumlular ile sorumlulukları incelenecektir. Buradan hareketle etkin bir Kurumsal Risk Yönetimi sisteminin nasıl kurulabileceği tartışılacaktır.

Anahtar Kelimeler: Risk, Risk Yönetimi, Kurumsal Risk Yönetimi, Sorumlular

JEL Kodları: D80, D81, G32.

1 Bu çalışma Emrah Erdem'in Kurumsal Risk Yönetiminde Çalışanların Risk Algısı: Bir Kalkınma Ajansı Örneğinde (Gazi Ün. Sosyal Bilimler Enstitüsü, Ankara, 2014) künyeli tezinden kısmen yararlanılarak hazırlanmıştır.

* Prof. Dr., Ankara Hacı Bayram Veli Ün. İİBF, Siy. Bil. ve Kamu Yön. Bölümü, mehmet.ozero@hbv.edu.tr, Orcid Id: 0000-0003-2220-2271

** Doktorant, Ankara Hacı Bayram Veli Ün. Lisansüstü Eğitim Enstitüsü, İşletme (Yönetim ve Organizasyon) A.B.D., emrherdm@hotmail.com, Orcid Id: 0000-0002-4321-7096

Yazı Gönderim Tarihi: 14.01.2022, Yazı Kabul Tarihi: 27.03.2022

ABSTRACT

In its most general form, risk management is to increase the development potential of an organization by managing the uncertainties and threats that it may encounter and be exposed to in the future in order to protect its customers (citizens, private sector and non-governmental organizations), personnel and itself. Enterprise Risk Management is the systematization of these studies within the organization based on the ERM framework. Both in English and Turkish, "risk" is defined as the degree of loss or damage or their probability. Both risk management and enterprise risk management are theorized over this concept. Enterprise Risk Management, which is the focus of the study, is a process that is structured throughout the organization and influenced by the board of directors, management and other employees, that identifies potential events that may affect the achievement of an organization's objectives, manages it within the limits of its willingness to take risks, and provides reasonable assurance that the organization's

objectives will be achieved. In this process, the most important elements within the scope of success criteria are all employees of the organization, especially senior managers. In the study, it is assumed that the effectiveness of Enterprise Risk Management depends on these responsible persons. In this direction, first the conceptual framework related to risk and risk management will be revealed, then Enterprise Risk Management, and in the last part, the organizational structure of this system in question, and those responsible and their responsibilities will be examined. From this point of view, how to establish an effective Enterprise Risk Management system will be discussed.

Keywords: Risk, Risk Management, Enterprise Risk Management, Responsibles

JEL Classification: D80, D81, G32.

1. GİRİŞ

Günlük hayatımızda sık sık karşı karşıya kaldığımız risk kavramı farklı kişilere farklı anlamlar ifade eder. Bu nedenle risk hakkındaki eylem ve düşünceler kişinin ait olduğu dünyanın algı ve değerlendirmelerinin sosyal ve kültürel yapılandırması ile öğrenilir. Burada devreye giren risk algısı ile belli bir kaza ya da tehlikeli olayın meydana gelme olasılığı ve bizi ne derecede ilgilendirdiği ya da endişelendirdiği ortaya konarak (Edward & Smith, 1907, s. 1) riskin önem derecesi belirlenir. Böylelikle birey tarafından duygusal sezgilerin tehlike ve risklerle ilgili bilgilerin alınarak benimsenmesi ve zihinde işlenerek, birey tarafından, olayların meydana geliş ve sonuçların şiddet olasılığının sezgisel olarak değerlendirilmesi mümkün olur (Hudspith, 2014, s. 1). Sonuçta tehlike ve şiddeti algılayan bireyler, karşılaşacakları risk durumu için önceden tedbir alma çabası içine girerler.

Genel olarak çoğu toplumda değerler bütünü; risk almaktan çok, "durağanlığı ve temkinliliği; belirsizlik toleransından çok verilmiş ilişkilerin devam ettirilmesini" içerir" (Bozkurt & Baştürk, 2009, s. 67). Toplumların sosyokültürel yapılarının risk ve riskin yönetimi süreçlerine doğrudan etkisi vardır.

Risk ve riskin yönetimi sürecini sosyokültürel etkenlerin yanında; "gönüllülük, kontrol edilebilirlik, aşinalık, adil olmak, avantajlar, dönülemez bir potansiyel, anlayış, şiddet ve belirsizlik, gecikmiş etkiler, mağdur kimlik, güven, kaza geçmişi ve etik/ahlak kodları da etkilidir. Bu unsurlar, insanlar genellikle "gerçek" zarar veya tehlike potansiyeli açısından daha fazla riski algıladıklarında" (Covello & Sandman, 2001, ss. 164-178) devreye girmektedir.

Risk ve riskin yönetimi ile ilgili bu hususlar, bu çalışmanın odağında yer alan Kurumsal Risk Yönetimi (KRY) için de doğrudan geçerlidir. Literatürde 2004 yılında Kurumsal Risk Yönetimi Çerçevesinin (COSO) yayımlanması ile KRY tüm dünya genelinde özellikle de gelişmiş ülkelere ses getirmeye başlamış ve bu gelişmelere hiçbir kuruluş kayıtsız kalamamıştır. KRY; "kuruluşu etkileyebilecek potansiyel olayları tanımlamak, riskleri kuruluşun risk alma profiline uygun olarak yönetmek ve kuruluşun hedeflerine ulaşması, finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ve uygulanabilir yasa ve düzenlemelere uygunluk amaçlarına ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; kuruluşun yönetim kurulu, yöneticileri ve tüm diğer çalışanları tarafından etkilenen ve

iç kontrolü de kapsayarak belirli bir strateji içinde tüm kuruluş çapında uygulanan sistematik bir süreç” (COSO, 2004, s. 4) olarak görülmektedir.

KRY, kuruluş içinde organize olmuş bir risk sistemi kurmayı hedefler. Hemen hemen tüm kuruluşlarda risk yönetiminin uygulanmasını zorunlu kılmak için kuruluşun uymakla zorunlu olduğu yönerge ve yönetmeliklere revizyon yapılmışsa da uygulamada yetersiz kaldığı bilinmektedir. Bu sebeple, öncelikle kuruluşlarda çalışan personelin günlük yaşantısında riskleri nasıl algıladığı ve yönettiğinin belirlenmesi gerekmektedir.

Bu süreçte ortaya çıkması olası sorunları en aza indirmek ya da önlemek için kuruluş içinde KRY sistem açıklarının belirlenerek etkin bir yapıya kavuşturulması gereklidir. Bunun için de KRY sistemini kurup, yaşatacak ve idamesini sağlayacak olan kuruluş çalışanlarının riski nasıl algıladıkları ve çözüm yolu buldukları algısının, KRY çalışmalarıyla ilişkili olup/olmadığının belirlenerek sistemin etkin bir hale dönüşümünü sağlamak gerekmektedir.

Uygulamada KRY, “gerekli kontroller ve dengelere dair temel ve geliştirilebilir bir yapı yoluyla kuruluşlara yardımcı olmaktadır” (Küçükylmaz, 2007, s. 65). KRY, “kuruluşlar ve ilgili tüm tarafları ile birlikte bugünün hızla değişen düzenlemeleri, piyasalar, finansal ve iş baskılarından kaynaklanan riskleri ve zorlukları yanıtlamalarında en iyi anlayışı, plan ve yönetim faaliyetlerini gerçekleştirme fırsatı vermektedir. Risklere ilişkin yanıt stratejilerinin geliştirilmesi ve yapılacak kontrollerin saptanması da KRY kapsamında gerçekleştirilmektedir”. Risk yönetimine yatırım yapıldığı takdirde, ölçülebilir faydasının en fazla olduğu sonuç, toplam maliyeti düşürücü (ARS, 2013, s. 60) etkisidir.

Bu çalışmada söz konusu kapsamda risk, risk yönetimi ve bunların sentezini oluşturan Kurumsal Risk Yönetimi konuları ele alınacaktır. KRY sürecinde sorumlular üzerinden hareket edilerek, sürecin başarı kriterleri değerlendirilecek ve daha etkin risk yönetimi uygulamaları için yapılması gerekenler tartışılacaktır.

2. RİSK VE RİSKİN YÖNETİMİ

Risk en basit şekliyle; gelecekte karşılaşılabilecek olan ve amaçların gerçekleştirilmesini engelleyebilecek tehditler/olumsuzluklar veya amaçlara ulaşmayı kolaylaştırabilecek fırsatlar olarak tanımlanmıştır (Derici vd., 2007, s. 1; İncesu, 2010, s. 4). Bu tanımla gelecekte ortaya çıkması muhtemel tehditleri olgunlaştırarak fırsat haline dönüştürmeyi ifade etmektedir. Şimdi bu tanımdan hareketle riski ve riskin yönetim sürecini ayrıntılı inceleyelim.

2.1. Risk Kavramı

Esas itibarıyla risk rastlantısal bir olayın meydana gelme olasılığıdır ve gerçekleştiğinde kuruluşun hedeflerine ulaşma başarısını negatif yönde etkiler (Kızıboğa, 2012b, s. 297). Risk kavramının bu tanım üzerinden kuruluşların gündeminde önemli yer işgal etmesi, söz konusu bu negatif etkiden kaynaklanmaktadır.

Bu nedenle kuruluşların gelecekte karşılaşılabileceği risklerin tespit edilmesi ve bu risklerin yönetilmesi son derece önem arz etmektedir. Haberleri izlediğimizde ekonomi kötü gittiğinde iflas eden şirketler, zarar açıklayan kuruluşlar ve performansının düşük olduğu görülen bazı kuruluşlar bu duruma örnek olarak verilebilir. Bu olaylardaki artış hızı, günümüz dünyasında risklerin tanınmasını ve risklere karşı tedbir alınmasını gerekli kılan, risk yönetimi kavramının önemini bir kez daha gözler önüne sermektedir. Bu sayede her kuruluş, ihtiyaçlarına uyacak farklı risklere odaklanabilmektedir (Kara & Sakarya, 2012, s. 71).

“Tüm risk türlerinde dikkate alınması gereken temel nokta, olayların gerçekleşme olasılıkları ile onların sonuçlarına dair fayda fırsatlarının veya başarı tehditlerinin farkına varılmasıdır. Bu yönüyle risk, kaçınılmazdır ve ortadan kaldırılamaz” (Küçükylmaz, 2007, s. 39).

Çalışma hayatında da tüm çalışanların “çabaları veya faaliyetleri belirsizlik ve risk içerir. Bu nedenle kuruluşların, herhangi bir kaynağın sebep olduğu krizlerle başa çıkmak için kendilerini hazırlamaları gerekir.

İdeal bir dünyada yöneticiler kötü olanı belirlemek ve krizin kaynağını tanımlayarak her biri için acil durum planı geliştirmek ister. Bu hazırlıklı olma fikrinin ilk adımdır. Krizler her zaman doğası gereği, sistemleri hazırlıksız bir şekilde yakalar” (Demirel & Taner, 2009, s. 128). Bu süreçte sorunları önlemek için ne yapılabileceğinin ayrıntılı olarak düşünülmesi gerekir. Olasılıkların gerçekleşme derecesini belirlemek ve başa çıkma yolları için çalışarak yeni sorunlara yanıt bulunulması günümüzün şartlarında temel bir zorunluluk olarak görülmektedir. Belirsizliklerin vereceği kaybı bertaraf etmek için, etkin bir risk yönetim sistemi gerekmekte, aksi halde uluslararası alanda sık sık örnekleri görülebilen krizler yaşanabilmektedir (Demirel & Taner, 2009, s. 128).

“Birey hayatında olduğu gibi kuruluşlar için de gelecekte karşılaşılabilecek olaylardan en az zarar ve en fazla fayda elde edebilmek, onları önceden fark edebilmeye ve onlar için en uygun eylemlerde bulunmaya bağlıdır” (Derici vd., 2007, s. 3). Risklerin kaynağı, kuruluşun faaliyet gösterdiği çevredeki belirsizlikler ve gelecekteki bilinmeyen olaylardır. Burada risk gelecekte olacak olayları ve getirileri sarmalayan bir belirsizlik durumunu betimler (Arslan, 2008, s. 18; Ogan, 2010, s. 9). Burada kişilerin, kuruluşların, sistemlerin ve devletlerin var oluş nedenlerini ve stratejilerini başarıyla yönetmelerini etkileyecek herhangi bir olayı risk olarak tanımlamak mümkün olacaktır (Küçükşahin vd., 2009, s. 12).

Risk, şu anda var olanlara değil gelecekte ortaya çıkma ihtimali olan şeylere işaret eder. Risk “zararlı veya istenmeyen bir şey olabileceği ihtimalidir. Yüz yüze gelinen yeni bir olay karşısında en doğru eylemlerde bulunmak, bu olayın olumsuzluklarını en aza indirip olumlu etkilerinden azami ölçüde istifade edebilmenin en iyi yolu, meydana gelmeden önce olayı tahmin etmek ve gerçekleşme ihtimali olanlara önceden hazırlık yapmaktır” (Derici vd., 2007, s. 21). Bu nedenle risk, geleceğe yönelik plan ve stratejilerimizi engelleyebileceğini düşündüğümüz etkileri bertaraf etmenin en önemli yolu olarak görülmektedir.

Tarihsel sürece baktığımızda Mezopotamya’da 3900 yıl önce başlayan sigorta uygulamalarının, risklerle başa çıkmak için uygulanan eski stratejilerinden biri olduğunu görüyoruz. M.Ö.1950’de Hammurabi,

gemilerin kayıp ihtimali için risk primi içeren sözleşmeler hazırlatmıştı. Yunanlılar da bu sözleşmeleri kullanmışlardır. İlk hayat sigortası poliçesi ise ancak 1583 yılında İngiltere’de uygulanmıştır (Molak, 1997, s. 18).

İtalyancası “Risco”, Almancası “Risiko”, Arapçası “Rızık”, İngilizcesi “Risk” olan bu kavramın kökeni Fransızca olup dilimize risk olarak yerleşmiştir. Gerek İngilizcede gerekse Türkçede “risk” kayıp hasar derecesi ya da kayıp, hasar derecesi olasılığı, sigorta edilen şey ya da kimse” olarak tanımlanmıştır (Özer, 2010, s. 211). Aşağıda literatürde risk ile ilgili kabul gören tanımlar yer almaktadır:

- En basit tanımı ile, kayıp ihtimalidir (Kızılboğa, 2012a, s. 96).
- Bir olayın doğurabileceği olumsuz sonuçların toplamını ifade eden kavramdır (Sönmez, 2013, s. 18).
- Kuruluşların hedeflerine ulaşmasını tehlikeye düşüren, beklenmedik olaylardır, gelecekteki olaylar ve sonuçları çevreleyen belirsizliktir, bir olayın doğurduğu olumsuz sonuçların toplamıdır ya da belirli bir büyüklükte meydana gelmesi halinde doğurabileceği kayıp olasılığıdır (Uzunçubuk, 2005, s. 18).

2.2. Risk Yönetimi

Risk yönetimi, kuruluşların kârlılık içerisinde faaliyetlerine devam etmesi için gerekli düzenlemeleri sağlamak, kuruluştaki mal ve kişilerin korunması ile işletmenin kazanma gücünü korumak; organizasyonda oluşabilecek beklenmeyen kayıpların en düşük maliyetle minimize edilmesi için gerekli olan kaynakların ve faaliyetlerin planlanması, yönetilmesi ve kontrol süreçlerini kapsamaktadır (Emhan, 2009, s. 209). Bu çerçevede muhtemel kayıplara maruz kalma olasılığını en aza indirmek için geliştirilen sistematik bir yaklaşımdır (Sung & Zhang, 2013, s. 677). Bir kişinin, bir proje veya firmanın, hedeflerine ulaşma sürecindeki belirsizliklerin tanımlanması, analizi ve etkilerinin değerlendirilmesi risk yönetimi sürecinde gerçekleşir (Tilki, 2013, s. 11). Yani risk yönetimi hedeflenen sonuca ulaşmak için başlangıcı ifade eder.

Tüm ülkelerde insanlar birçok riske maruz kalır (Jina, 2014, s. 55). Risk yönetimi gelişimi ile bu süreç paralellik taşımaktadır. Risk yönetimi geliştiği takdirde yetersizlik, belirsizlik, yoksulluğun azaltılması ve ekonomik büyümenin sağlanması da dahil olmak üzere kalkınma hedeflerine daha kolay ulaşmak için yetersizlikler ortaya konularak problemler ve belirsizliklerin kaynağına kadar inilme fırsatı sağlanmış olur. Burada gerçek risk yönetiminin önemi (Cendrowski & Mair, 2009, s. 6), bugünün rekabetçi ekonomi dünyasında daha belirgin hale gelmiştir. Risk yönetimi anlayışı, fırsatlardan azami ölçüde istifade etmek ve tehditleri en aza indirmek, yani risklere karşı yapabileceklerimizin mantığını ve yöntemlerini bize sunmaktadır (Derici vd., s. 1). Bu şekilde risk yönetimi hayatımızın vazgeçilmez (Cendrowski & Mair, 2009, s. 1) bir ögesi haline hızla dönüşmektedir.

Risk yönetimi; riskleri tanımlamayı, değerlendirmeyi, onlara karşı yürütülecek faaliyetleri belirlemeyi, sorumlulukları tayin etmeyi, belirlenen faaliyetleri uygulamayı ve bunları izlemeyi ve sonuçlarını gözden geçirmeyi kapsayan bütün süreçlerdir (Derici vd., 2007, s. 3). Olumlu ve olumsuz yönleri ile giderek gelişen bir olgudur. Genel olarak kuruluşlar bu durumun olumsuz yönleri ile ilgilenerek riski önleme ve hafifletmeye odaklanmışlardır (Airmic, 2012, s. 1). İyi bir risk yönetimi odağı bu risklerin tanımlanması ve tedavi edilmesi üzerine odaklanmalıdır.

Riskler tanımlanırken risk algısı devreye girmektedir (Sha vd., 2001, s. 348). Risk yönetimi sürecinde dikkat edilmesi gereken algılamayı etkileyen faktörlerden bazılarını da şu şekilde belirtebiliriz (Schmidt, 2004, s. 3):

- Gönüllülük: Bu durumda risk algısı düşecektir. Zorlama olduğu takdirde ise algı yükselecektir. Gönüllü olan kişi riski her zaman durduracağına inanır.
- Kontrol Edilebilirlik: Algılanan risklerin kendi kontrolünde olması risklerin kabul edilmesini sağlayacaktır. Çalışanlar kontrol dışı olan riskleri kabullenmezler.
- Gecikme Etkisi: Gecikme fiziksel, kimyasal veya biyolojik nitelikte olabilir. İlk olay ve

gecikmeli etki arasındaki ilişki hemen belli olmayabilir. Çünkü gecikme etkisi belli bir risk etkisini tanımda ek güçlüklerle neden olmaktadır. Bu duruma örnek olarak sigara sebebi ile akciğer kanserine yakalanmak, dengesiz beslenme ile kalp hastası olmak gösterilebilir. Genetiği değiştirilmiş ürünler ve bunların potansiyel çevresel etkileri de bu duruma örnek verilebilir. Risk algısının geç oluşmasını sağlayacak nedenlerin etkisi düşünülerek riskler belirlenmelidir.

- Doğal ve Yapaylık: Risk hakkında bilgi sahibi olunması gerekir. Risk ya da zararın suni veya doğal olup olmadığı risk algısında fark yaratır. Suni hasar daha temkinli ve ihtiyatlı davranışlar ile önlenabilir, ya da riskli konu hakkında daha fazla bilgi sahibi olunmasını gerektirir.
- Aşinalık ve Alışkanlık: Bilinmeyen ve yeni birçok riske sahibiz. Risk kabul etmekle başlar ve riske yavaş yavaş alışmayı gerektirir. Uzun bir süre için mevcut olan bir teknik risk aynı kalmış olsa da alışkanlık nedeniyle zayıflatılmaktadır. Bilinen riskler bilinmeyenlere göre daha fazla kabul edilir. Maruz olma veya olmamanın belirsizliği aşinalığı etkiler.
- Fayda ve Risk-Fayda Dağılımı: Adil dağıtılacak algılanan riskler, haksız dağıtılacak algılanan risklerden daha fazla kabul görür. Bu durumda risk eşit dağıtılacak (herkes risk taşır) ancak sadece bir birime fayda sağlayacaktır. Personelin bu durumdan olumlu etkilenmesi için risk dağıtımından sağlanan faydanın, riski alanlara dağıtımının hakkaniyetli yapılması gerekir.

Görüldüğü gibi en kısa şekliyle risk yönetimi, bir kuruluşun müşterilerini, personelini ve kendisini koruması için uyması gereken prosedürlerdir. Kuruluşun hedeflerine ulaşmasını engelleyecek risklerin ve fırsatların belirlenerek, risklerin değerlendirilmesine ve yönetilmesine ortam hazırlar. Ayrıca, kabul edilebilir risk toleransları içinde kuruluşa yönelik tehdit ve fırsatlarını yönetmek olarak da (Ferma, 2014, s. 1)

görülen risk yönetimi herhangi bir kuruluşun stratejik yönetiminin merkezi bir parçasıdır. Organizasyonun stratejisi ve bu stratejinin uygulanması boyunca sürekli çalışan ve gelişen bir süreç (Airmic, 2012, s. 2) niteliğindedir.

Günümüzde risk yönetimi hızla gelişen bir disiplindir ve öngördüğü uygulamaların ne için ve nasıl olacağı ile ilgili bir çok görüş bulunmaktadır (Kimbrough, 2006, s. 18). Bugün küreselleşmenin hızla geliştiği dünyamızda, işletmelerin faaliyet gösterdiği ulusal ve uluslararası çevrede önemli değişimler yaşanmakta; ekonomik, siyasal, sosyal, teknolojik, yasal ve endüstriyel koşullar hızla farklılaşmakta, kuruluşlar kıyasıya bir rekabet ortamına girmektedirler (Harmankaya, 2012, s. 54). Küreselleşme, çok büyük fırsatlarla birlikte, ölümcül riskleri de beraberinde getirmiştir. Böyle bir ortamda ise sektör ayırt etmeden, her kuruluş kendi çapında risk yönetimine ihtiyaç duyar hale gelmiştir (Güneş & Teker, 2010, s. 64).

Bu tür ortamlarda; riskleri tanımlamayı, değerlendirmeyi, onlara karşı yürütülecek faaliyetleri belirlemeyi, sorumlulukları tayin etmeyi, belirlenen faaliyetleri uygulamayı ve bunları izlemeyi ve sonuçlarını gözden geçirmeyi kapsayan (İncesu, 2010, s. 6) risk yönetimi uygulamaları bütüncül bir sistem olarak kuruluşların gündemine girmiştir. Kuruluşlar, risk yönetimi stratejisine sahip değiller ise, hızla bu konuda kendilerini geliştirmeye başlama gereğine inanmışlardır. Kuruluşlar ayrıca risk yönetiminin, bunu benimseye hazır olan personel için bir verimlilik anahtarı olduğunun da bilincindedirler.

Risk yönetimi kuruluşlarda değer oluşturur ve bu değerleri de korur. Organizasyon ve karar verme süreçlerinin ayrılmaz bir parçasıdır. Açıkça belirsizliği giderir. Sistemattir, yapılandırılmıştır ve böylelikle zamanı tam kullanır. Mevcut en iyi bilgiye dayanır. Kuruluşun içinde olduğu duruma özel olarak tasarlar. Bu süreçte insani ve kültürel faktörleri dikkate alır. Her daim şeffaf ve kapsayıcı olmak zorundadır. Bu ortamda dinamik, tekrarlı ve değişime duyarlıdır. Bu nedenle kuruluşun sürekli gelişimini kolaylaştırır (Crawford, 2012, s. 9). Literatürde ayrıca risk yönetimi uygulamasının katkıları; sürpriz ve kayıpları en aza indirmesi, hızlı ve etkili karar almaya yardımcı olması, zaman tasarrufu sağlama, kaynak israfını

önlemesi, risklerin makul seviyelerde tutulmasını sağlama ve kişileri, yeniliklere açık olma hususunda cesaretlendirmesi şeklinde de belirtilmektedir (Derici vd., 2007, s. 3). Günümüzde başarılı organizasyonlar belirsizlik ortamından kaçınma yollarını aramak gibi bir çaba yerine risklerden fırsatlar elde etmeye odaklanmışlardır (Akçakanat, 2012, s. 36). Bunun sonucu olarak da geleneksel bakış açısıyla uygulanan risk yönetimi mevcut koşullarda yetersiz kalmakta ve organizasyonel, stratejik ve kurumsal bir risk yönetimi uygulamasına ihtiyaç duyulmaktadır.

Risk yönetiminin tarihsel gelişimine baktığımızda hemen hemen bütün kaynaklar sigortacı Edward Lloyd'u işaret etmektedir. 1667'de Edward Lloyd Londra'da bir kahve dükkânı açmış ve bu dükkânı zamanla gemicilikle ilgili bilginin değiş tokuş edildiği bir merkez haline getirmiştir. 1696'da Lloyd Listesinin oluşturulması ile bu bilgi aktarımı resmi bir boyut kazanmıştır. Böylece Lloyd'un kahve dükkânı dünyanın denizcilik sigortasının merkezi olarak gelişmiştir. Zamanla Lloyd daha büyük risk havuzları oluşturarak ve risklerin kapsadığı alanları genişleterek tüm sigortacılık sektöründe lider konumuna gelmiştir (Arslan, 2008, s. 23; Kızılboğa, 2012b, s. 83).

1963 yılında, ilk risk yönetimi makalesi "Risk Yönetimi ve İşletme" başlığıyla yayımlanmıştır. Bu dönemde Petrol İhraç Eden Ülkeler Örgütü (OPEC) fiyat artırmak amacıyla üretimini azaltmaya karar vermiş, bu süreçte petrol fiyat artışı, döviz kuru ve enflasyon oranındaki istikrarsızlık, finansal risk yönetimi uygulamalarını zorunlu olarak gündeme getirmiştir. Uzun bir süre sigorta sektörü ile eş anlamlı kullanılan risk yönetimi kavramı 1970'lerde Amerika'da iş dünyasında geniş kabul görmeye başlamıştır. Bretton Woods anlaşmasının sona ermesi ve 1973 petrol krizi sonucunda risk oranlama ve değerlendirme danışmanlık hizmeti talepleri artmaya başlamıştır (Cendrowski & Mair, 2009, s. 1).

Bu dönemde görüldüğü gibi risk yönetimi uygulamaları en fazla Amerika Birleşik Devletleri'nde küreselleşmeye yanıt olarak gelişmiştir. Daha sonra 1980'li yıllarda, farklı ülkelerde farklı siyasal rejimlerin bir sonucu olarak politik riskler, çok uluslu şirketler tarafından dikkate alınmaya başlanmıştır. Bu dönemde hükümetler yeni politikalarını açıklayarak yatırımcı-

ların ve şirketlerin riskini azaltmak için teşvik edici uygulamalar yapmışlardır. Bu süreçte risk yönetimi metotları ve yöntemleri, önce likidite, kredi ve operasyonel risk olarak başlatılmış (Lou & Heitger, 2005, s. 6) daha sonra alanı genişletilmiş, tüm faaliyetlerde düşünülmesi ve çalışılması gereken bir olgu haline dönüşmüştür.

Görüldüğü gibi son yıllarda risk yönetimi uygulamaları, sadece tehlike riskleri ile değil aynı zamanda finansal, operasyonel ve stratejik riskler kapsamında da gündeme gelmiştir. Risk yönetiminin çok fonksiyonlu bir olgu olarak ele alınması gerekliliği böylece ortaya çıkmıştır (Kızılboğa, 2012/b, s. 299). Böylelikle risk yönetimi, piyasadaki artan rekabetten doğan risklerin değerlendirilmesi ve kuruluşların büyümesini hedefleyen iş risk yönetimine (Arslan, 2008, s. 23) doğru kaymaya başlamıştır. Risk yönetiminin bütün kamu kuruluşlarında başarılı bir şekilde uygulandığı İngiltere’de, 1994 yılında Hazine tarafından yayınlanan Risk Yönetimi Rehberi esas alınarak risk yönetimi uygulaması başlatılmıştır.

Bu şekilde modern anlamda risk yönetimi tabiri ilk kez 1950’li yılların sonlarında Amerika Birleşik Devletleri’nde kullanılmaya başlanmıştır (Emhan, 2009, s. 212). İlk risk yönetimi makalesi yukarıda belirttiğimiz gibi “Risk Management and Business Enterprise” başlığını taşımakta olup, Robert I. Mehr ve Bob Hedge tarafından yazılmış ve 1963 yılında yayımlanmıştır (Cendrowski & Mair, 2009, s. 1). Bu çalışmada öncelikle risk yönetiminin amacının kuruluşun üretici etkinliğini maksimize etmek olduğuna (Küçüküylmaz, 2007, s. 42) vurgu yapılmıştır.

Doğaldır ki ülke uygulamalarındaki risk yönetim sisteminin amacı aynı, ancak uygulama modeli ülkeden ülkeye farklılık gösterebilmektedir. Bu alanda en fazla dikkat çeken uygulamalar ABD, Kanada, Avustralya, Yeni Zelanda ve İngiltere risk yönetim modelleri (Kızılboğa, 2012a, s. 83) kapsamında hayata geçirilmiştir. Son yıllarda özellikle Avustralya, Yeni Zelanda ve İngiltere’de risk yönetim alanında ön plana çıkmaya başlamışlardır.

3. KURUMSAL RİSK YÖNETİMİ (KRY)

Yukarıda da belirttiğimiz gibi esasında riskleri belirlemek ve değerlendirmek için kuruluşlar için en kapsamlı yöntem, tanımlama ve değerlendirme, yapılandırılmış bir kurumsal risk (ARS, 2013, s. 62) yönetimi sürecinde gerçekleşir. Kurumsal Risk Yönetimi (KRY) “kuruluşun amaçlarına ulaşmasını etkileyen risklerin belirlenmesinde, analizinde, önem sırasına göre sıralandırılmasında ve belirlenen risklere karşı önemli hedefleri, ilgili projeleri ve günlük faaliyetleri göz önünde bulundurarak gerekli tepkinin verilmesinde, kuruluşun büyüklüğüne ve görevine bakmaksızın, tüm işletmeleri kapsamlı ve sistematik bir şekilde ele alan bir yaklaşımdır. Burada KRY, kuruluşlarda ortaya çıkan belirsizlikleri etkin bir şekilde yönetme yeteneğini geliştirmeyi hedeflemektedir” (Küçüküylmaz, 2007, s. 54). Şimdi bu modeli daha ayrıntılı inceleyelim.

3.1. Kurumsal Risk Yönetiminin Tanımı ve Kapsamı

Kurumsal risk yönetimine ilişkin COSO Treadway Komisyonuna göre en yaygın kabul görmüş tanım şöyledir, s. “Kurumsal Risk Yönetimi; kuruluşu etkileyebilecek potansiyel olayları tanımlamak, riskleri kuruluşun risk alma profiline uygun olarak yönetmek ve kuruluşların hedeflerine ulaşması, finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ve uygulanabilir yasa ve düzenlemelere uygunluk amaçları ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; kuruluşun yönetim kurulu, yöneticileri ve tüm diğer çalışanları tarafından etkilenen ve iç kontrolü de kapsayarak belirli bir stratejide tüm kuruluş çapında uygulanan sistematik bir süreçtir” (COSO, 2004, s. 4).

KRY sistemi, stratejilerin oluşturulması ve kuruluş çapında uygulanması, kuruluşu etkileme olasılığı olan olayların belirlenmesi, risklerin risk iştahı kapsamında yönetilmesi ve kuruluş hedeflerine ulaşmasına yönelik güvence sağlar. Böylelikle kuruluşlar bir organizasyonun karşı karşıya kaldığı tüm riskleri yönetmek için sistematik ve tutarlı bir yaklaşım benimsemeye odaklanır. Daha sade bir tanımla KRY, “kuruluşun hedeflerine ulaşmasına ilişkin güvence sağlayan, risk iştahı içinde risklerini yöneten, tüm süreçle-

rinde etkili olmasını sağlayan tanımlanmış potansiyel riskleri baştan aşağı gözden geçiren, strateji belirleyen, yönetim, yönetim kurulu ve diğer personel tarafından kuruluş genelinde işbirliğiyle gerçekleştirilen bir süreçtir” (ERM, 2004, s. 4).

Diğer bir tanımda ise KRY, bir kuruluşun hedeflerine ulaşmasını etkileyebilecek potansiyel olayları tanımlayan, risk alma istekliliği sınırları içinde yöneten ve kuruluş hedeflerinin başarılması konusunda makul derecede güvence sağlayan, kuruluş genelinde yapılandırılmış ve yönetim kurulundan, yönetimden ve diğer çalışanlardan etkilenen bir süreçtir (Pehlivanlı, 2022, s. 3).

KRY'nin temel ilkeleri, stratejik planlama, finansal uygulama ve uygulama faaliyetlerinden kaynaklanan riskler için kurumsal yönetim sağlayarak, herhangi bir varyasyonu ölçme ve adresleme için bir karar verme süreci olarak gündeme gelmiştir (Connolly, 2004, s. 23). Bu kapsamda kurumsal risk yönetimi, kuruluş içinde devam eden bir süreç olarak kabul edilir. Organizasyonun her seviyesinde insanlar tarafından etkilenen, strateji belirleyen, her düzeyde ve birimde, işletme genelinde uygulanan, risk iştahı içinde riski yönetmek, potansiyel olayları tanımlamak, bir kuruluşun yönetimi ve yönetim kuruluna makul güvence sağlamak, bir veya daha fazla ayrı ama üst üste gelen kategorilerde bulunan hedeflerin gerçekleştirilmesi için (ERM, 2004, s. 4) tasarlanmaktadır.

Görüldüğü gibi KRY devamlı bir süreçtir. Bu hedefler belirlenmesi ve risklerin belirlenmesi ile başlar (Products, 2013, s. 8). Riskler belirlenirken değişen şartlar dikkate alınmalıdır. Kuruluşlar; küreselleşme, teknoloji, düzenlemeler, yeniden yapılanma, değişen pazarlar ve rekabetin belirsizlik yarattığı bir çevrede faaliyet göstermektedirler (Küçükylmaz, 2007, s. 33). Küreselleşme açısından bakıldığında, hızlı büyüyen teknolojik bağımlılığın (Razali & Tahir, 2011, s. 12) artması riskleri çeşitlendirmiştir.

3.2. Kurumsal Risk Yönetimi'nin Kuruluşlara Faydaları

KRY'nin amacı kayıpları azaltarak, risk ve fırsatla karşı karşıya olan insanların (WDR, 2014, s. 62) gelecekteki beklentilerine cevap verebilmektir. Buna ek

olarak, kuruluşların risk ve fırsatları yönetebilmesini sağlayan risk yönetim sistemini; kuruluşa değer katmak, geliştirmek ve kaynakların en etkin şekilde kullanılmasını sağlayarak kuruluş hedeflerine ulaşmasını (Kızılboğa, 2012b, s. 8; Pehlivanlı, 2022, s. 3) kolaylaştırmaktır. Bu kapsamda hedeflerin başarılması için belirsizlikleri yöneterek kuruluşları canlı tutmaya, korumaya ve geliştirmeye çalışır (Ontario, 2011, s. 6). KRY, kuruluş yönetimlerine belirsizlikler ve onunla birleşmiş risk ve fırsatlarla, değer oluşturma kapasitesini artırma yoluyla etkin ve verimli bir yapı sağlamaktadır (Küçükylmaz, 2007, s. 88).

KRY faaliyetleri; risklerinin yönetimi ile ilgili kuruluşun beklentilerini özetleyen bir politika geliştirmek, süreci belgelemek ve analiz yapmaya olanak sağlamak, öğrenme sürecine yardımcı olmak için kuruluş için özel risklerin belirlenmesini sağlamak, kurumsallaşmış KRY sistemini etkili bir şekilde yerleştirmek, analitik araçlar ve öneriler geliştirmek, risk ve fırsat yönetimi için kritik konulara farklı bakış açıları aramak, sistemin doğru algılanması sağlanarak örgüt kültürüne bütünleştirilmesini sağlamak (Hardy, 2010, s. 8) amaçlarıyla yürütülür.

Kuruluşlar için KRY; olası mali kayıpları azaltmak için örgüt arzusu, iş performansını artırmak için organizasyon arzusu, yasal uyumluluk gereksinimleri nedeniyle, risk hesap verebilirliği artırmak için organizasyon arzusu oluşturmak amacıyla (Razali & Tahir, 2011, s. 12) gerçekleştirildiği için büyük önem taşır. KRY sayesinde stratejik-üst düzey hedefleri ile uyumluluk sağlanır ve ilgili görevler desteklenir. Kaynakların etkin ve verimli kullanımı, raporlama güvenilirliği ve yürürlükteki kanun ve düzenlemelere kolay uyum sağlanır (ERM, 2004, s. 4).

KRY, kuruluşlara; istenen sonucun elde edilmesine güven duyulması, tehditlerin kabul edilebilir seviyede sınırlanması, fırsatlardan yararlanma konusunda elde edilen gerekli bilgiye dayanarak kararlar alınması, paydaşların kuruluşun yönetimine ve hüküm verme yeteneklerine olan güvenlerinin artması (Arslan, 2008, s. 21) gibi kolaylıklar sağlar. Ancak bu faydaların elde edilebilmesi için risk yönetimi, belirli bir birimde veya fonksiyonda değil, kuruluşun genelinde bir bütün halinde yürütülmelidir (Arslan, 2008, s. 24).

Görüldüğü gibi risk yönetimi, kuruluşlara birçok fayda sağlar, tehlikelerden korur ve hedeflerini destekleyerek organizasyon ve paydaşlarına aşağıda belirtilen katkıları sağlar (Airmic, 2012, s. 4):

- Gelecekteki faaliyetleri gerçekleştirecek bir organizasyon için bir çerçeve sağlanması tutarlı ve kontrollü bir şekilde gerçekleşir.
- Faaliyet, dalgalanma ve proje fırsat / tehdit kapsamlı ve yapılandırılmış bir anlayış ile karar verme, planlama ve önceliklendirme iyileştirmesi sağlar.
- Gerekli olmayan alanlarda değişkenlik azaltılır.
- Varlık ve firma imajı korunur ve artırılır.
- Kişi ve kuruluşun bilgi tabanı geliştirilir hatta ilgili süreçler bu doğrultuda desteklenir.
- Operasyonel verimliliği optimize etmek çok daha kolaylaşır.

Bunların yanında risk yönetimi faaliyetleri kuruluşların farkındalık kültürünün oluşturulmasına da yardımcı olur (Cendrowski & Mair, 2009, s. 22). “Temel KRY faydaları teorik olarak kurumsal yaklaşım, organizasyonel verimlilik, proaktif tutum, raporlama, iç denetim fonksiyonu, iş performansı ve kurumsal yönetim alanlarını kapsayacak şekilde belirlenmiştir” (Küçükylmaz, 2007, s. 92). Bu doğrultuda KRY organizasyonun performansını artırarak; değişikliklere hazır olma durumunu geliştirir. Operasyonel kayıpları azaltır. Düzenlemelere uyum ve risklere cevap vermeyi mümkün kılar. Performans hedefleri ile ilgili belirsizliklerin tahmin edilmesini sağlar. Sistematik risk değerlendirme sürecine güven sağlar. Fazla ve gereksiz faaliyetleri ortadan kaldırır. Risklere uygun verilen cevapları bir araya getirir. Risk işlem maliyetini düzenler. Riskin ne kadarının tolera edileceğini belirler (Akçakanat, 2012, s. 3).

3.3. COSO Kurumsal Risk Yönetimi Modelinin Gelişimi

2000’li yıllarda ABD’de büyük kayıplara neden olan iş skandalları, ekonominin yavaşlamasının işlerde ka-

yıplara neden olması ve dünyadaki gelişmelerin yeni riskleri ortaya çıkarması ile herkes risk yönetiminin önemini farkına vardı. Bu dönemde yapıların uyumsuzluğu nedeniyle farklı alanları kapsayan risk yönetimi modellerinin bir arada kullanılması birçok soruna yol açtı. Bu durum riski tartışmak, tanımlamak, değerlendirmek ve yönetmek için ortak bir model oluşturulması gereğini ortaya koydu. Böyle bir modelin oluşturulması projesine COSO (Committee of Sponsoring Organizations-Sponsor Olan Kurumlar Komitesi) tarafından 2001 yılında başlandı. Çalışma birçok kaynaktan edinilen bilgilerle geliştirildi, birçok farklı tarafı temsil eden birçok kişiden anketler ve diğer yöntemlerle görüşler alındı ve bu sayede edinilen bilgiler de modele girdi oluşturdu. COSO ’nun yetki verdiği bir danışma kurulu da sürece katkı sağladı ve rehberlik etti. 2004 yılı sonunda model tamamlandı (Arslan, 2008, s. 26) ve kamuoyuna duyuruldu.

Bu kapsamda kuruluşlar; “finansal ve operasyonel risklerinin yanı sıra etik, sosyal ve çevresel riskler de dahil olmak üzere, karşı karşıya oldukları tüm iş risklerini tanımlama ve onları makul seviyelerde tutacak şekilde nasıl yönettiklerini açıklama konularında yükümlülük altına girdiler. Bunun sonucu olarak da KRY; birçok kuruluş tarafından stratejik, finansal, operasyonel tüm risklerin belirlenmesine ve yönetilmesine, karşılaşılan ekonomik belirsizlikler karşısında dayanıklılık, sürdürülebilirlik ve esneklik elde edilebilmesine imkân sağlayan bir araç olarak gündeme geldi” (Akçakanat, 2012, s. 44). COSO böylelikle KRY Çerçevesini, çoğunlukla aşağı yönlü risklerin yanı sıra, uyum ve raporlama yönetmek için de (Faris, Gilbert & LeBlanc, 2013, s. 2) kullanmaya başladı.

COSO KRY Çerçevesinin dikey bileşenleri; kontrol ortamı, hedef belirleme, olay tanımlama, risk değerlendirme, risk tutumu, kontrol faaliyetleri, bilgi ve iletişim ile izleme faaliyetlerinden meydana gelmektedir. Ayrıca çerçevede amaçlar kategorisi stratejik, operasyonel ve mali raporlama ve uygunluk şeklinde sınıflandırılmıştır. Bu kapsamda amaçlar kategorisini oluşturan riskleri şu şekilde açıklayabiliriz (Faris, Gilbert & LeBlanc, 2013, s. 3-6):

- Stratejik Riskler: Kuruluşların sürdürülebilirlik konularında dikkatli davranması gerekir. Genellikle bu riskler neyin yanlış gide-

bilir olduğuna odaklanan yönetim sistemleri üzerinde yönetilirler. Kuruluş yöneticisi neyin doğru gittiği hakkında proaktif düşünüyor olmalıdır.

- Operasyonel Riskler: İş operasyonları içerikleri son 5-10 yılda önemli ölçüde değişmiştir. Örneğin Japonya'da 2011 yılında Fukushima depremi ve tsunamisi, 2012 yılında Sandy kasırgası operasyonel risklerin önemini bir daha ortaya koymuştur. Birçok kuruluş artık bir ürünün yaşam döngüsü değerlendirmesini yapmak ve müşterilerine bu bilgiyi sağlamak zorundadır. Operasyonel risk kapsamında, sürdürülebilirlik faktörlerinin genellikle kurumsal itibar ve iş sonuçları üzerinde orantısız büyük etkisi bulunmaktadır.
- Uygunluk Riskleri: Birçok şirket, yeni gündeme gelen çok sayıda yeni ve genişleyen yasal uyum riskleri ile karşı karşıyadır. Düzenleyici önlemler almak için doğrudan veya dolaylı olarak çıkan önemli risk alanları; sağlık, güvenlik, insan hakları, iş yasaları, anti-rüşvet ve çevresel riskler gibi oldukça farklı olabilmektedir.
- Risk Raporlama: Giderek büyüyor olan kuruluşlar sürdürülebilirliği tercih ediyorsa daha şeffaf olmalıdırlar. Sürdürülebilirlik raporları, kuruluş organizasyonunu iyi anlamanıza yardımcı olur. Son yıllarda kamu kuruluşları da sürdürülebilirlik uygulamalarını dikkate almış ve daha şeffaf olma yolunda ilerlemeler kat etmişlerdir.

3.4. Kurumsal Risk Yönetimi, İç Kontrol ve Denetim

Risk yönetimi, birçok unsuru açısından iç kontrol sisteminin bir parçasıdır. Başka bir ifadeyle, KRY'nin bütünsel parçasıdır. Burada iç kontrol; belirlenen hedef ve amaçlara ulaşılması, kaynakların etkin ve verimli kullanılması, kuruluşların faaliyetlerinde yer alan yapısal risklerin uygun bir biçimde kontrol edilmesi, mali ve diğer yönetim bilgilerinin güvenilirliğinin, doğruluğunun, yasalara, yönetmeliklere, stratejilere, planlara, iç kural ve prosedürlere uyumunun

sağlanması amaçlarını gerçekleştirmeye çalışan bir süreçtir (Arslan, 2008, s. 42).

İç kontrol sisteminin daha rutin konuları içermesine karşılık, risk yönetimi, daha ileriye dönük, üst düzey ve kuruluş dışına da yönelik stratejiler ve daha genel politikalar içermesi nedeniyle çok fonksiyonlu bir yapıya sahiptir. Risk yönetiminde risklere karşı en doğru kontrol faaliyetleri belirlenir ve en iyi şekilde uygulanır. Elbette ki bu, öncelikle risklerin tam ve doğru olarak tespit edilmesi, sorumluların tayin edilmesi, sürecin işleyiş mekanizmalarının oluşturulması, işlemin izlenmesi ve gözden geçirilmesi aşamalarını gerektirir (İncesu, 2010, s. 13; Derici vd., 2007, s. 22).

KRY kuruluş genelinde olan ve strateji oluşturma sırasında yerleştirilen; kuruluş yönetim kurulu, yönetimi ve diğer personelinin etkilenen; kuruluşun hedeflerine ulaşmasına yönelik makul bir güvence sağlamak için onu etkileyebilecek potansiyel olayları tanımlamak ve risk kapasitesi içinde yönetmek amacıyla tasarlanmış bir süreçtir. Kuruluşun varlığının nedeni belirli hedeflere ulaşmaksa, iç kontrol bunu başarmak için kuruluşa rehberlik eder ve risk yönetimi de kuruluşun hedeflerine ulaşmasına engel olacak olaylara müdahale ederek kuruluşun rotasından çıkmasını önler. İç kontrol ile faaliyetlerin uygun tarzda yapılması sonucunda, iyi kurumsal yönetiminin amacı olan sürdürülebilir kuruluş performansı yoluyla değer yaratma, koruma ve artırma hedeflerine ulaşılır (Küçükylmaz, 2007, s. 80).

İç kontrol gibi iç denetim de son yıllarda bu doğrultuda yön değiştirmiş, geçmişle ve sadece kontrollerle ilgilenmek yerine geleceğe ve gelecekte kuruluşu bekleyen risklere odaklanmaya başlamıştır (Kara & Sakarya, 2012, s. 71).

Risk yönetimi, kontrol ve yönetim alanlarında güçlü sistemler oluşturamayan kuruluşlar, uzun vadede başarısız olacaklardır. Üç yıllık olarak tasarlanan iç denetim planları, kuruluşun faaliyetlerinin ve karşı karşıya olduğu risklerin kapsamlı bir incelemesi ve analizi yapıldıktan sonra hazırlanır. Kuruluş için en yüksek riski oluşturan faaliyetler, coğrafi bölgeler, özel projeler, iş süreçleri ve iştirakler; düşük riskli alanlara göre iç denetimin dikkatinin daha çok olduğu alanlardır. Yüksek riskli alanlar, düşük riskli alan-

lara göre daha sık iç denetime tâbi tutulur (Tufan & Görün, 2013, s. 121).

Bu kapsamda hazırlanan denetim standartları; politika ve prosedürlerin oluşturulması, kamu sektörü denetçilerinin risk değerlendirmesi yapmalarında ve raporlama sorumluluklarını yerine getirmelerinde değerli bilgiler sağlayabilir. Bir denetimde veya denetim sınıfında olağan dışı risklerin veya durumların tespit edilmesi ve denetim sırasında belirlenen önemli riskler ve bu risklere karşı yapılacak işleri kapsar.

28945 Sayılı Riskin Erken Saptanması Sistemi ve Komitesi Hakkında Denetçi Raporuna İlişkin Esaslara Yönelik İlke Kararına göre (KGK, 2014); “denetçinin amacı, riskin erken saptanması ve yönetimi sistemine yönelik bir değerlendirmenin doğasından kaynaklanan kısıtlamalar sebebiyle denetçinin, yaptığı denetim çerçevesinde, sistem tarafından bütün risklerin doğru bir şekilde tespit edilip edilmediğini ortaya konulmasıdır. Bu şekilde kuruluşun varlığını, gelişmesini ve sürekliliğini tehdit edebilecek muhtemel risklerin zamanında tespiti, analizi ve ilgili birimlere bildirimlerin (komite tarafından yönetim kuruluna yapılan raporlamalar dâhil), yönetimin bu risklere uygun bir karşılık vermesine imkân sağlayacak şekilde zamanında yapılıp yapılmadığı belirlenir. Denetçi, kuruluşun; finansal raporlama amaçlarıyla ilgili iş hayatına ilişkin risklerin belirlenmesi, risklerin öneminin tahmin edilmesi, bu risklerin gerçekleşme ihtimallerinin değerlendirilmesi, bu risklere karşı atılacak adımlara karar verilmesine ilişkin bir sürecinin bulunup bulunmadığı gibi hususlar hakkında bilgi edinir. Denetçi uygulanacak müteakip denetim prosedürlerini tasarlarlarken her bir işlem sınıfı, hesap bakiyesi ve açıklama için yönetim beyanı düzeyindeki önemli yanlışlık riskine ilişkin değerlendirmenin aşağıdakileri de içeren gerekçelerini dikkate alır:

- İlgili işlem sınıfı, hesap bakiyesi veya açıklamanın belirli özellikleri sebebiyle önemli yanlışlık bulunması ihtimali (yapısal risk),
- Risk değerlendirmesinin ilgili kontrolleri dikkate alıp almadığı (kontrol riski); dolayısıyla, kontrollerin etkin biçimde işleyip işlemediğine karar vermek amacıyla denetçinin denetim kanıtı elde etmesinin gerekip gerekmediği,

- Yaptığı risk değerlendirmesi sonucunda belirlediği risk düzeyi ne kadar yüksekse, o kadar fazla ikna edici denetim kanıtı elde etmesi.”

4. KURUMSAL RİSK YÖNETİMİ VE GENEL YÖNETİM SÜRECİ

Örgüt kültürü ve kontrol ortamının diğer kuruluşlar için de oluşturulabilmesi için risk yönetimi sistemlerini kamu otoritesi adına sahiplenen, süreci izleyen ve ilgili kuruluşları raporlama fonksiyonu ile takip eden bir üst kurula (bağımsız idari otoriteye) ihtiyaç vardır (Pehlivanlı, 2022, s. 7). Yönetim kurulu seçimi ve üst düzey yöneticilerin değerlendirilmesi ile; planlama, performans izleme, strateji ve risk denetlemek; yöneticileri dengeleme, kurumsal politika ve planlarını onaylamak; işin olağan akışı içinde maddi sermaye harcamalarını onaylama; bütünlüğün ve şeffaflığının sağlanması, yürürlükteki kanun ve yönetmeliklere uygunluk denetiminin sağlanması (Cendrowski & Mair, 2009, s. 14) ile gerçekleştirilir. Kuruluşun tüm üyeleri, organizasyonun her düzeyinde önemli konularda yönetime girdi sağlamak için sürece (Duckert, 2011, s. 28) dahil edilmelidir.

Değişimin ve gelişimin bir sonucu olarak artan belirsizlik ortamında, çalışanlar, belirli ölçülerde risk alarak hareket etmek durumundadırlar. Risk alma, girişimci yöneticilerin önde gelen özelliklerinden biridir. Belirsizliğin doğurduğu bilgi yetersizliği nedeniyle zamanında verilmeyen kararlar, kuruluşların fırsatları kaçırmalarına sebep olabilir. Rekabet avantajını kaybedebilirler. Belirsizlik altında çalışanlar, uygun şekilde risk alarak karar vermelidirler (Kurt, 2012, s. 33). Bu da ancak, yönetim kademesinin KRY sistemini tam anlamı ile kabullenmiş olması ve tüm personelin katılımı ile etkin bir çalışma ortamının yaratılması ile gerçekleştirilebilir.

4.1. Kurumsal Risk Yönetimi'nde Organizasyon Yapısı

KRY sürecinde yöneticiler, öncelikle riskin etkin yönetiminden danışmanların belirlediği risk seçenekte-

ri arasından tercih yapmaktan, elde edilecek faydaya göre riski kabul veya reddetmekten, risk yönetimi konusunda çalışanların eğitilmesi ve teşvik edilmesinden, etkisini aşan risk kararlarını daha üst seviyelere, uygun karar verme organlarına iletmekten sorumludurlar (Özer, 2011, s. 347).

Risk yönetimi değişiminin karmaşıklığı ve hızı artıyor (ARS, 2013, s. 82) olmasına rağmen, organizasyonda uygun risk yönetimi yapısı ile değişime cevap vererek karşılaşılabilecek negatif durumların pozitif çevrilmesi sağlanacaktır. Kuruluş yöneticileri, kurumsal risk yönetimi sürecini değerlendirmek, güçlendirmek ve hedefe doğru yönlendirilmesini sağlayacak (ERM, 2004, s. 9) en etkili kademedir. Yöneticiler, süreçleri ve kaynakların daha etkin yönetimi için yeni yollar bulabilir ve en iyi uygulamaları bulmak için sorumluluğu (Hardy, 2010, s. 9) alması gerekebilir. Çünkü yirmi birinci yüzyılın yöneticisi, risk yönetimini çok iyi bilmek ve uygulamak zorundadır (Özer, 2010, s. 211).

-Yönetim Kurulunun Sorumluluğu: Günümüzde yönetim kurulları için risk yönetimi uygulamaları açısından kuruluş büyüklüğü veya türü güçlü bir odak noktası olmaya devam etmektedir (ARS, 2013, s. 8). Üst yönetim kurulu, kuruluşun kurumsal risk yönetim durumunu tartışmak ve gerekli gözetimi sağlamaktan sorumludur. Yönetim kurulu, etkili bir kurumsal risk yönetimini sağlamanın yanı sıra, en önemli risklerden de haberdar olmalıdır. Yönetim kurulu, iç denetçiler, dış denetçiler ve diğer girdi arayanları da dikkate almalıdır (ERM, 2004, s. 9). Etkin yönetim kurulu üyeleri, objektif, yetenekli ve sorgulayıcıdır. Yönetim kurulunun şirketin stratejik yönünü tayin etme ve risk yönetimi içeriğini oluşturma sorumluluğu vardır. Yönetim kurulunun risk yönetimi sorumlulukları; riskin stratejik bakış açısını belirleme ve risk iştahı ayarlama, risk yönetimi yapısını kurma, en belirgin riskleri anlama, kuruluşu kriz anında yönetme olarak sayılabilir. Kurul belirli iş risklerini değerlendirir ve anahtar riskleri düzenli bir güncelleştirmeye tabi tutar (ARS, 2013, s. 74). Yöneticiler, uygulamanın risk toleranslarıyla uyumlu olmasını sağlayarak, kendi sorumluluk alanlarındaki KRY parçalarının uygulanmasını yönlendirirler (Küçükylmaz, 2007, s. 134).

Bu kapsamda yönetim kurulunun başlıca sorumlulukları; kuruluşun stratejik yönünü belirlemek ve etkin çalışması ve risk yönetimi için bir çerçeve oluşturmak, kabul edilemez risklerin nasıl yönetilmesi gerektiğini belirlemek, olumsuz risklerin kuruluş üzerindeki etkisini en aza indirilmek, risklerin fayda ve maliyetlerinin kontrolünü üstlenmek, risk yönetim sürecinin etkinliğini sağlamak (Airmic, 2012, s. 12), risk iştahı seviyelerini belirlemek, KRY faaliyetlerini denetlemek, maruz kalınmış önemli risklerin niteliğini ve büyüklüğünü belirlemek, belirlenmiş stratejik risk hedefleri için risk seviyelerini karşılaştırmada ilgili raporları değerlendirmek, risk yönetimi ve risk iştahı politikalarının uygun ve ihtiyatlı kalmasını sağlamak (Ontario, 2011, s. 13) olarak sayılabilir.

-Üst Yöneticinin Sorumluluğu: Üst yönetici, kuruluşun niteliğine göre, başkan, yönetim kurulu başkanı, genel müdür ve benzeri unvanları taşıyabilecek olan kuruluşun en üst düzeydeki yöneticisidir (Derici vd., 2007, s. 14). Üst yönetici, kuruluşun KRY yeteneklerini değerlendirmek zorundadır. Bu kapsamda daha derinlemesine değerlendirme olup olmadığını belirlemesi gereklidir (ERM, 2004, s. 9). Üst Yönetici KRY yetenekleri ve etkinliğinin değerlendirmesini görüşmek üzere iş birimi yöneticileri ve önemli personellerini bir araya toplayarak fikirlerine başvurur. “Belirli süreçlerdeki, operasyonlardaki ya da bölümlerdeki yöneticilere belirli KRY uygulamaları için sorumluluk verir. Bu yöneticiler, olayların belirlenebilmesi ve risk değerlemesi için teknikler geliştirirler. Birimin hedeflerine yönelik risk prosedürlerinin geliştirilip uygulanmasında ve hammadde satın alması ya da yeni müşterilerin kabul edilmesiyle ilgili kuralların geliştirilmesi gibi karşılıkların belirlenmesinde rol oynarlar” (Küçükylmaz, 2007, s. 134).

-Yöneticilerin Sorumluluğu: Üst yöneticilerin sorumluluğu “KRY’nin tüm parçalarının yerinde olduğunu gözetmektir. Üst düzey yönetici, diğer yöneticilere liderlik ve yön sağlayarak, satış, pazarlama, üretim, satın alma, finans, insan kaynakları gibi önemli operasyon alanlarından sorumlu üst düzey yöneticilerle periyodik olarak toplanarak, riski nasıl yönettikleri de dahil olmak üzere sorumluluklarını gözden geçirerek görevlerini yerine getirirler. KRY sürecinin

oluşturulması kararı sonrası yapılması gereken ilk iş bir risk yönetimi lideri atanmasıdır” (Özer, 2012, s. 144). Kuruluşun büyüklüğüne bağlı olarak risk yönetim işlevi tek bir risk savunucusu, yarı zamanlı bir risk yöneticisi, tam ölçekli risk yönetimi bölümü gibi değişebilir (Airmic, 2012, s. 12). Kurumsal risk yöneticisinin sorumlulukları; risk yönetimi stratejisini ve politikasını belirleme, stratejik ve operasyonel düzeyde risk yönetiminin birincil savunucusu olma, kuruluş içinde risk farkındalığı oluşturulması için eğitim verme, iş birimleri için risk politika ve yapıları kurma, risk yönetimi için süreçleri tasarlama ve gözden geçirme, kuruluş içinde risk yönetimi konularında tavsiyelerde bulunma, çeşitli fonksiyonel faaliyetleri koordine etme, acil durum ve iş sürekliliği programları hazırlama, risk tepki süreçlerini geliştirme, yönetim kurulu ve paydaşlar için risk raporları hazırlama, önemli stratejik, iş ve süreç risklerini tanımlama, ölçme, değerlendirme (Ontario, 2011, s. 14) olarak belirtilebilir.

-Finansal yöneticilerin, İç ve Dış Denetçilerin Sorumluluğu: KRY sorumlularına bakıldığında “finansal yöneticilerin ve çalışanlarının çok önemli pozisyonda oldukları görülür. Finansal yöneticiler hedeflerin oluşturulmasında, stratejilerin belirlenmesinde, risklerin analiz edilmesinde ve kuruluşu etkileyen değişikliklerin nasıl yönetileceği konusunda karar verilmesinde, vazgeçilmez bir görev üstlenirler. Çok değerli bilgiler sağlarlar, yön gösterirler ve karar verilen aksiyonların izlenmesi ve takip edilmesi sağlayacak bir pozisyonda bulunurlar” (Küçükylmaz, 2007, s. 137).

İç denetçiler de KRY'nin etkinliğinin değerlendirilmesinde ve düzeltmelerin önerilmesinde önemli rol oynarlar. İç denetçi KRY sürecinde üst yönetime risk alma istekliliği seviyelerinin belirlenmesinde, risklerin ölçülmesinde ve etkili bir şekilde kuruluş politika, süreç ve uygulamalarına dönüştürülmesinde danışmanlık sağlayabilirler veya güvence hizmetini üstlenebilir. İzleme faaliyetini de gerçekleştirirler (Pehlivanlı, 2022, s. 6). İç denetçiler, KRY olgunluk seviyesi ve organizasyon itibarıyla kendilerine biçilen sınırlar dahilinde risk tanımlama aşamasında aktif görev alabilecekleri gibi sürecin etkinliğinin denetiminden de sorumlu tutulabilirler. İç denetçiler, risk değerlendirme ve

risklerin sıralama faaliyetini güvence verme fonksiyonu çerçevesinde incelerler. Önemli riskler hakkında iç denetim çalışmalarına odaklanarak, yönetim tarafından tanımlanan ve risk yönetim süreçlerinin denetimini yapmak, risk yönetimine güvence sağlamak, risk yönetimi sürecinde aktif destek ve katılımını sağlayarak risk tanımlama/değerlendirmesini kolaylaştırmak ve risk yönetimi ve iç kontrol hat elemanı yetiştirmek, yönetim kurulu ve denetim kuruluna koordine risk raporlama, yapmak gibi (Airmic, 2012, s. 13; Ontario, 2011, s. 14) temel görevleri vardır. İç denetçiler, risk etki ve olasılıklarının ölçümünde kullanılan araçların kalitesini sorgularlar ve risklerin tam olarak değerlendirilip değerlendirmediği hakkında güvence verirler. Bu aşamada raporlanan anahtar riskleri değerlendirmeleri gerekir. Bu kapsamda kurul ve denetim komitesine verilen risk raporlarını koordine ederler (Kara ve Sakarya, 2012, s. 76). İç denetçiler kuruluşun kontrol yapısını değerlendirirken mali denetim, uygunluk denetimi, performans denetimi ve sistem denetimi uygulamalarını yaparlar (Akçakanat, 2012, s. 43).

Kuruluşlarda risk ve kontrol kültürü oluşturulurken örgüt kültürü ile bütünlük sağlanması, altyapı donanımının sağlanması ve çalışanların bilgi ve yeteneklerin belirlenmesi gerekmektedir (Aydeniz, 2008, s. 14). Kuruluşların sahip oldukları en büyük değer insan gücü olduğu bir gerçektir. Teknolojideki gelişmeler nedeniyle büyük ve hızlı olursa olsun kuruluşların insana ve onun yaratıcılığına olan ihtiyacı hiçbir zaman önemini yitirmeyecektir. Bu ise var olan bir gerçeği bir kez daha gözler önüne sermektedir; başarı ancak sahip olunan bilgi ve yetenekler potansiyelini, belirlenen hedefler doğrultusunda harekete geçirmek ve onu en etkin şekilde kullanabilmekle mümkün (Doğan, 2007, s. 15) olabilmektedir.

Neredeyse tüm çalışanlar risk yönetimini etkilerler. Risklerin belirlenmesi ya da değerlendirilmesinde kullanılan bilgileri oluşturabilir ya da KRY'yi etkilemek için gerekli diğer faaliyetlerde bulunabilirler. Bu faaliyetlerin özenle gerçekleştirildiği bir kuruluşta bu durum KRY'nin etkinliğini doğrudan etkiler. Tüm personel, KRY'nin içinde bulunan bilgi ve iletişim akışını desteklemekle sorumludur. KRY herkesin işidir ve tüm çalışanların rolleri ve sorumlulukları açıkça tanımlanmalı ve etkin bir şekilde bildirilmelidir (Küçükylmaz, 2007, s. 139).

Kuruluşlarda yukarıda belirtilenler dışında kalan diğer personelin gün bazında riski yönetmek için birincil derecede sorumluluğu vardır. İş birimi yönetimi, risk yönetim hedeflerini tanıtmak ve risk bilincini teşvik etmekle sorumludur. İş birimi yönetimi, kavramsal projelerin yanı sıra proje boyunca risk yönetiminin de dahil edildiğinden emin olmalıdır (Airmic, 2012, s. 12). Bunun yanında dış denetçilerin de KRY'de sorumluluğu vardır. Dış denetim dış denetçiler tarafından yapılan denetimi ifade eder. Dış denetçiler, denetim yaptıkları kuruluşla ilişkisi olmayan yani organizasyondan bağımsız olan denetçilerdir. Dış denetimin, risk yönetim sisteminin yapısını anlaması, kontrol riskinin değerlendirilmesi sürecinde önemli veriler sağlar. Burada kontrol riski, denetim riskinin önemli bileşenlerinden biridir. Denetçiler, kuruluşun kontrol yordamlarını gözlemleyerek, belgeleri inceleyerek, yönetimi ve çalışanları sorgulayarak KRY sistemini izlerler (Akçakanat, 2012, s. 45). Dış denetçiler yönetim ve yönetim kuruluna, bağımsız ve objektif bir bakış açısı sağlarlar. Bu durum diğer amaçlar kadar kuruluşun dış finansal raporlama amaçlarını başarmasına da katkıda bulunabilir. KRY ve kontrolündeki eksikliklerle ilgili bulguları bildirme yoluyla dikkatleri çekmek ve geliştirilmesine dair tavsiyeler sunmak (Küçükylmaz, 2007, s. 39) en önemli sorumluluklarındandır.

4.2. Kurumsal Risk Yönetimi'nde Başarı İçin Kritik Faktörler ve Etkinlik

Etkin KRY sistemine geçişin başlatılabilmesi için atılması gereken ilk adım; herkesin bu konuda aynı kavramlarla düşünmesine yönelik ortak bir dilin oluşturulmasını sağlamak ve risk yönetim rol ve sorumluluklarını açığa kavuşturarak, yönetime güvenirliliği arttırmak amacıyla idareden destek (Arslan, 2008, s. 50) almaktır. Bir risk uygulayıcının ilk olarak katılımın kapsamını belirlemek için bir risk yönetimi stratejisi belirlemesi önemlidir (Cendrowski & Mair, 2009, s. 13). Bu stratejiyi belirlerken kuruluş özelliği, çalışma alanı, dış etmenler, iç etmenler ve üst yönetimin tutum ve davranışı sürece dahil edilerek yol haritasının çıkarılması önem arz etmektedir.

Risk yönetim süreçleri içinde olan insan unsuru ve prosedürleri bir kuruluşun kültüründe önemli bir etkidir. Risk yönetimi kültürünün en önemli bileşenlerinden biri olan hesap sorgulama, KRY felsefesidir. Risk yönetimi merkezli bir kuruluşun tüm seviyelerinde hesap verilebilirlik sorumluluğu kurulması gerekir. Hesap verebilirlik olmadan çalışanların, risklerin bilincinde olması mümkün değildir (Cendrowski & Mair, 2009, s. 20).

Literatürde KRY 'de başarı için en yaygın kritik faktörler aşağıda sıralanmıştır (Hardy, 2010, s. 9):

- KRY için kısa ve uzun vadeli stratejik planlar kurulması,
- KRY'yi kabul ederken, faydaların paydaşlara iletiğinden emin olunması,
- Diğer kuruluşlarla karşılıklı işbirliği içinde olunması,
- “Tekerleği yeniden icat etmeyin” anlayışının tüm aktörlerce kabullenilmesi,
- KRY vizyonunu başarmak için deneyimli ve nitelikli personele sahip olunması,
- Kuruluşun en altı ile en üstü arasında iletişimin güçlü olmasının sağlanması.

Risk yönetiminde etkin olabilmek için yukarıda bahsettiğimiz gibi yöneticiler bu süreçte önem taşımaktadırlar. Kişisel olarak riski, algılama, öngörme, sezme, gerekli tedbirleri hızlı bir şekilde alabilmek gibi kişisel yeteneklere sahip olan yöneticiler, riskin her türlüünün yönetiminde çok daha başarılı olmaktadır (Özer, 2012, s. 160). Kurumsal risk yönetimi bir süreçtir. Bu sürecin başarıya ulaşması; kuruluş genelinde sağlam bir yapının oluşması, insan odaklı kararlar alınması ve stratejik hedefler doğrultusunda KRY'nin etkinleştirilerek belirsizlik ortamından fırsat ve kazanç ortamına geçiş yapılması ile gerçekleştirilecektir.

Uygulamada risk yönetimi araştırmaları, riskin ne kadar erken teşhis edilip müdahale edilirse, o kadar projenin başarısızlığının ve maliyet kaybının önlenmesi olasılığının yüksek olduğunu göstermektedir. Risk yönetimi, olumsuz şoklara karşı kuruluş dayanıklılığını arttırabilmek için önemli roller üstlenmektedir (Erdem & Younis, 2012, s. 4).

KRY sistemi geleneksel risk yönetimindeki gibi riskleri “kötü olumsuz” olarak algılamaz. Riskleri yönetilebilir ve kuruluş için artı bir değere dönüştürülebilir gözüyle değerlendirdiğinden, hedeflere yönelik riskler tanımlanarak, nasıl tutumlara uygulanabileceği belirlenir ve böylelikle gözden kaçan fırsatların farkına varılır. KRY sistemi kuruluşun başarısız sonuçlara değil, süreçte başarısız sonuçların ortaya çıkmasına sebep olan nedenlere odaklanılmasını ve onların yönetilmesini ve hatta fırsat sağlayıcı durumların ortaya çıkarılmasını sağlamaya odaklanır (Kızılboğa, 2012a, s. 312). Kuruluşu tehdit eden durumun tanımlanarak ve değerlendirilerek fırsat haline dönüştürülmesi ancak KRY anlayışı ile gerçekleştirilebilir. Eğitim, KRY için sorumluluk sağlayan önemli bir araç olarak hizmet edebilir. Sürekli ve doğru eğitim politikaları ve prosedürlerinin uygulanması doğru karar almayı destekler (Green, 2013, s. 34). KRY sisteminin, kuruluşun hedeflerine ulaşma başarısını artırmasına ve kuruluşa değer katarak gelişim sürecini desteklemesine önem verilmelidir (Kızılboğa, 2012b, s. 96).

Uygulamada KRY'nin etkili olması için; kuruluş üst yönetiminin desteği, kuruluş içinde sorumluların atanması, eğitim ve gelişim için uygun kaynakların tahsisi ve tüm paydaşlar tarafından risk bilincinin geliştirilmesi (Airmic, 2012, s. 12) gerekir. Ayrıca etkili bir KRY uygulanması; gözetim (tüm kritik riskler; tanımlanmış, yönetilmiş ve izlenmiş olmalıdır), sorumluluk (riskin; tanımlanması, değerlendirilmesi, hafifletilmesi ve raporlaması için sorumlular, yönetim tarafından atanmalıdır), güvence (yöneticiler riskin belirli seviyede yönetildiğine güvence vermeli) (Ontario, 2011, s. 5) şeklinde belirtilen hedeflere ulaşmak için kuruluş üst yönetimleri yoğun çaba harcamalıdır.

5. SONUÇ

Çalışmada genel olarak değerlendirdiğimiz gibi risk yönetiminin kuruluş stratejisinin etkin bir şekilde uygulanmasını destekleyecek sürekli bir süreç olarak geliştirilmesi (Airmic, 2010, s. 6) gerçeği artık tüm kuruluşlarda kabul edilen temel bir yönetim anlayışına dönüşmüştür. Kuruluşların kârlı ve verimli bir organizasyon yapısına kavuşmak için yönetim stratejisi

oluşturarak dahili ve harici tüm risklerin üstesinden gelmesinin (Brannan & Taylor, 2006, s. 2) değişen dünyanın kaçınılmaz zorunluluğu olduğu gerçeği, bugün KRY'nin hızla gelişiminde temel bir itici faktör olmuştur. Bu nedenle günümüzde gerek özel sektörde gerekse de kamu sektöründe kuruluşlar bu modeli kurabilmek için yoğun çaba harcamaktadırlar.

1990'lı yılların sonunda ABD başta olmak üzere dünya genelinde yaşanan şirket skandalları, kuruluşların daha adil ve şeffaf yönetilmesini destekleyen kurumsal yönetim anlayışını ve bu anlayışı destekleyici, kuruluşun geneline uygulanabilen KRY sistemine ilişkin taleplerin artmasını sağlamıştır (Kızılboğa, 2012a, s. 297, 2012b, s. 84). 2000'li yıllarda ABD'de büyük kayıplara neden olan yönetim skandalları, ekonominin yavaşlamasının işlerde kayıplara neden olması ve dünyadaki gelişmelerin yeni riskleri ortaya çıkarması ile herkes risk yönetiminin öneminin farkına varmıştır (Ogan, 2010, s. 8). Bu dönemle beraber dünya genelinde KRY uygulamaları hızla artmış ve yaygınlaşmıştır.

Gerek özel sektör gerekse de kamu sektörü kuruluşları; ekonomik, teknolojik, politik, pazar ve rekabet çevrelerindeki belirsizlik arttıkça bir takım risklere maruz kalırlar (Çakınberk, 2010, s. 354). Değişen dünya nedeni ile kuruluşların hata yapma olasılığı ve hataların maliyetleri sürekli artmaktadır. Önümüzdeki dönemde risk yönetim fonksiyonuna sahip kuruluşlar ve buralarda görev alan risk yöneticilerinin sayısı kuşkusuz ki artacaktır. Eğer başarıların tesadüfi olması istenmiyorsa, değişen koşullar ve dinamikler altında dahi her koşulda başarı sürdürülmek isteniyorsa (Saka, 2010, s. 18), klasik risk yönetimi anlayışından kurumsal yapının esas alındığı KRY anlayışına geçilmesi gerekmektedir. Kurumsal riskleri azaltmak ve klasik risk yönetimine kıyasla iş kollarında veya birimler arasında iletişim kurmak, teknikler kullanmak ve entegre bir sistem kurmak (Razali & Tahir, 2011, ss. 8-16) için KRY sistemine ihtiyaç duyulur. Çalışmada sık sık vurguladığımız gibi KRY, organizasyon içinde riskleri yönetmede sistematik bir disiplin yaklaşımıdır. Birimler arası iletişimi güçlendirir. Bilgi alışverişini kolaylaştırır, yaygınlaştırır. Kuruluş içinde örgüt kültürü oluşmasını sağlar ve iyi yerleşmiş örgüt kültürü de risk yönetimi tabanlı karar verme üzerinde etkili olur.

Bugün, karşı karşıya olduğumuz en önemli gerçeklik değişimdir. Bu durum önemini tüm dünya tarihi içerisinde son 60 yılda çok hızlı artmıştır. Klasik risk yönetim sisteminin dar kapsamından çıkarılarak kuruluşların her türlü faaliyet alanında karşılaşılabilecekleri riskleri (stratejik, faaliyet, uygunluk, raporlama, teknolojik ve personel gibi) ele alabilecek şekilde genişletilmesi artık bir zorunluluk haline gelmiştir.

Risk yönetiminin önemi arttıkça klasik risk yönetimi yöntemlerinin; riski tanımlama, değerlendirme ve yönetmede yetersiz olduğu görülmüştür. Bu klasik yöntemler, kuruluşun hedeflerine ulaşmasını kolaylaştırmak ve değer yaratma sürecine katkıda bulunmaktan çok, kayıpları engellemeye yönelik olduğundan çoğu kuruluş risk yönetimini yeniden tanımlamak zorunda kalmışlardır.

Son yıllarda risklerin çeşidi ve miktarı artmakta ve çözüm üretme ihtiyacı bir zorunluluk olarak hem kuruluş yöneticilerinin hem de kamu kuruluşlarının karşısına devamlı olarak çıkmaktayken bu zorluğun üstesinden gelmek ve KRY uygulamalarına yön vermek amacıyla COSO tarafından çeşitli çerçeve metinler yayımlanmıştır. KRY uygulamalarını başlatmak isteyen ya da mevcut çalışmalarını yeniden yapılandırmak isteyen kuruluşlar açısından bu mevzuat büyük katkı sunmuştur.

Bugün ilginçtir ki, KRY için tüm bu uygun zemine rağmen; kuruluşlar “finansal ve operasyonel risklerinin yanı sıra etik, sosyal, iç ve dış çevresel riskler de dahil olmak üzere, karşı karşıya oldukları tüm iş risklerini tanımlama ve onları makul seviyelerde tutacak şekilde nasıl yönettiklerini açıklama konularında yetersiz kalmaktadırlar. Bunun sonucu olarak da KRY, kuruluşlar tarafından stratejik, finansal, operasyonel tüm risklerin belirlenmesi ve yönetilmesi için ekonomik belirsizlikler karşısında dayanıklılık, sürdürülebilirlik ve esneklik sağlamak amacıyla benimsenmektedir” (Akçakanat, 2012, s. 15). Söz konusu süreçte, başta COSO olmak üzere tüm aktörler KRY sistem ve uygulamalarının daha da rasyonel hale getirilip kuruluşlara maksimum fayda sağlamaları için üzerlerine düşen görevleri yerine getirmek zorundadırlar. Aksi halde dünya, riskini yönetemeyen, başarısız olmuş, iflas etmiş kuruluşlar “çöplüğüne” dönecektir.

Kaynakça

- Akçakanat, Ö. (2012). Kurumsal risk yönetimi ve kurumsal risk yönetim süreci. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 4 (7), 30-46.
- Arslan, I. (2008). *Kurumsal risk yönetimi*. Maliye Bakanlığı Strateji Geliştirme Başkanlığı.
- Aydeniz, Ş. (2008). *Risk yönetimi*, Denizli: Arıkan Basım Yayım Dağıtım.
- Bolgün, E. (2010). *Küresel krizin nedeni risk yönetimi mi?* İzmir: İzmir Ekonomi Üniversitesi Yayınları, 35.
- Bozkurt, V. ve Baştürk, Ş. (2009). Kobi girişimcilerinde risk ve belirsizlik algıları: Bursa örneği, *Ankara Üniversitesi SBF Dergisi*, 64(2), 43-74.
- Brannan, W. L. & Taylor, J. R. (2006). *A model for enterprise risk management within a healthcare organization*. Web: <http://www.asse.org/practicespecialties/riskmanagement/docs/Brannan%20&%20Taylor%20Article.pdf> Son Erişim Tarihi: 10.11.2013.
- Çakınberk, A. (2010). Stratejik ittifaklarda risk faktörleri ve risk yönetimi. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 20(1), 353-366.
- Cendrowski, H. & Mair, W. C. (2009). *Enterprise risk management and COSO*, Canada, 1. Web: http://www.cca-advisors.com/PDFs/Risk_Management_preview.pdf Son Erişim Tarihi: 10.06.2014.
- Connolly, J. (2004). The newest buzz at companies? “Risk management on steroids”. *National Underwriter Life & Health*, 108(39), 23.
- Covello, İ. & Sandman, P. M. (2001). *Risk Communication: Evolution and Revolution*, John Hopkins University Press, 164-178. Web: <http://www.psandman.com/articles/covello.htm> Son Erişim Tarihi: 08.03.2014.
- Crawford, M. D. (2012). *An exploration of enterprise risk management maturity factors within transportation organizations*, the degree of Master of Science, University of Colorado, Colorado.

- Demirel, E. & Taner, B. (2009). Risk yönetiminde riske maruz değer yöntemleri ve bir uygulama. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(3), 127-148.
- Derici, O., Tüysüz, Z. & Sarı, A. (2007). Kurumsal risk yönetimi ve Sayıştay uygulaması. *Sayıştay Dergisi*, 65, 151-172.
- Doğan, H. (2007). İşletmeler de örtülü bilginin somutlaştırılması ile olası stratejik risk sendromlarına ilişkin çözüm önerileri. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 9 (2), 143-160.
- Duckert, G. H. (2011). *Practical enterprise risk management: A business process approach*, John Wiley & Sons, ABD, 35.
- Emhan, A. (2009). Risk yönetim süreci ve risk yönetmekte kullanılan teknikler. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 23(3), 209-220.
- Erdem, O. A. & Younis, A. E. (2012). Yazılım projelerinde risk yönetimi. *Bilişim Teknolojileri Dergisi*, 5 (1), 1-5.
- Faris, C., Gilbert, B. & LeBlanc, B. (2013). *Integrating the triple bottom line into an enterprise risk management program*, Miami University, USA, 2.
- Gren, H. (2013). *The relationship between organizational risk management and job satisfaction in law enforcement*. the Degree of Doctor, Walden University.
- Güneş, Ş. & Teker, S. (2010). Türk enerji sektöründe kurumsal risk yönetimi farkındalığı. *Doğuş Üniversitesi Dergisi*, 11 (1), 64-76.
- Hardy, K. (2010). *Managing risk in government: An Introduction to enterprise risk management*, IBM Center for The Business of Government, 10.
- Harmankaya, D. B. (2012). Risk yönetimi ve işletmelerde uygulanabilirliği, *Verimlilik Dergisi*, 54, 41-59.
- Hudspith, B. (2014). Risk perception and risk acceptance: Implications for nuclear energy. Web: <http://www.nuceng.ca/sner/acceptance.pdf> Son Erişim Tarihi: 05.01.2014.
- İncesu, E. (2010). Kurumsal Risk Yönetiminde, Seydişehir Devlet Hastanesi Risk Yönetim Modeli Uygulaması. 5. Uluslararası Sağlıkta Kalite, Akreditasyon ve Hasta Güvenliği Kongresi Tam Metin Kitapçığı, Antalya.
- Jina, A. (2014). Risk management can be a powerful instrument for development, *World Development Report*, 55.
- Kara, S. & Sakarya, Ş. (2012). Kurumsal risk yönetimi çerçevesinde risk odaklı iç denetim ve İMKB uygulaması. *Muhasebe ve Vergi Uygulamaları Dergisi*, 65-86.
- Kimbrough, R. L. (2006). *The relationship between perceptions of organizational culture and implementation of enterprise risk management*, The Degree Of Doctor Of Philosophy, Alabama.
- Kızılboğa, R. (2012a). Risk yönetimi ve ülke uygulamalarında risk yönetim modelleri. *Akademik Araştırmalar ve Çalışmalar Dergisi*, 4(7), 82-99.
- Kızılboğa, R. (2012b). Geleneksel risk yönetiminden kurumsal risk yönetim sistemine geçiş. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16(3), 297-316.
- Küçükşahin, A., Şafak, İ. C. & Dedeoğlu, Ç. (2009). Güvenlik bağlamında risk ve risk yönetimi. *Güvenlik Stratejileri Dergisi*, 5(10), 9-35.
- Küçükylmaz, A. (2007). *Havaalanlarında kurumsal risk yönetimi: Atatürk havalimanı terminaleri işletmesi için kurumsal risk yönetimi model önerisi* (Yayımlanmamış doktora tezi). Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.
- Kurt, D. (2012). *Vekalet teorisi çerçevesinde hisse senedi maaş yapılarının risk alma davranışı ve finansal performans etkisi: S&P 500 firmaları üzerine bir uygulama* (Yayımlanmamış doktora tezi). Yıldız Teknik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Lou, B. & Heitger, D. (2005). A Building-Block approach for Implementing COSO's enterprise risk management—integrated framework, *Management Accounting Quarterly*, 6(2), 6.
- Molal, V. (1997). *Risk analysis and risk management*. Lewis Publishers, 17.

- Ogan, E. (2010). *Küresel kriz ve risk yönetimi: Yeni finansal yapı ve beklenen riskler*. İzmir Ekonomi Üniversitesi Yayınları, 9.
- Ontario (2011). Enterprise Risk Management Framework, Web: http://www.documents%20and%20Settings/ UltraXP/Belgelerim/Downloads/DICO_ERM_Framework_September_2011.pdf Son Erişim Tarihi: 10.06.2014.
- Özer, M. A. (2010). *Kuruluşlarda süreç, performans ve risk analizi/yöntemi*. Ankara: Adalet Yayınevi.
- Özer, M. A. (2011). *21. Yüzyılda yönetim ve yöneticiler*, Ankara: NOBEL Akademik Yayıncılık.
- Özer, M. A. (2012). Rekabet ortamında girişimciler için var olabılme reçetesi: Risk yönetimi. *Girişimcilik ve Kalkınma Dergisi*, 7(1), 143-162.
- Pehlivanlı, D. (2022). *Kurumsal risk yönetimi uygulamaları*, İstanbul: Asil Denetim, Web: <https://sertifikaliicdenetici.files.wordpress.com/2012/09/kurumsal-risk-yc3b6netimi.pdf> Son Erişim Tarihi: 13.03.2022.
- Products (2013). Risk and policy management Web: www.scmagazine.com/uk Son Erişim Tarihi: 05.01.2014.
- Razali, A. R. & Tahir, I. M. (2011). Review of the literature on enterprise risk management. *Business Management Dynamics*, 1 (5), 9-14.
- Saka, T. (2010). *Yeni-Dünya ekonomik düzeninde risk yönetiminin rolü*. İzmir Ekonomi Üniversitesi Yayınları, 35.
- Schmidt, M. (2004). Investigating risk perception: A short introduction, Austria, 3. Web: http://faculty.mercer.edu/butler_aj/documents/Intro_risk_perception_Schmidt.pdf. Son Erişim Tarihi: 03.05.2014.
- Sha, H., Arkam, M., Hussain, M., Imran, S. & Rehman, K. U. (2011). Relationship between risk perception and employee investment behavior, *Journal of Economics and Behavioral Studies*, Vol. 3, No. 6, 348.
- Smith, E. J. (1907). New York Times. Web: <http://www.is-sagligi-ve-guvenligi.com/makaleler/risk-degerlendirme/158-risk-algisi-nedir.html> Son Erişim Tarihi: 12.06.2014.
- Sung, M. C. & Zhang, J. (2013). Risk management capability building in SMEs: A social capital perspective, *International Small Business Journal*, 67, 670-689.
- Tilki Bostancı, H. (2013). *Firma düzeyinde riske karşı duyarlılığın beklenti teorisi ile açıklanması* (Yayımlanmamış doktora tezi). Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.
- Tufan, M. & Görün, M. (2013). Türkiye'deki kamu iç denetim sisteminin uluslararası iç denetim standartları çerçevesinde incelenmesi. *Sayıştay Dergisi*, (89), 115-135.
- Uzunçubuk, L. (2005). *Yerleşim yerlerinde afet ve risk yönetimi* (Yayımlanmamış doktora tezi). Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Whitman, M. E. & Mattord, H. J. (2012). *Principles of information security*. United States of America, 594.

İnternet Kaynakları

- AIRMIC (2010). *A structured approach to enterprise risk management and the requirements of ISO 31000*, 6. Web: <http://www.e-finance.com/RaportyCIMA/6.pdf> Son Erişim Tarihi: 05.03.2014.
- AIRMIC (2012). *The Association of Insurance and Risk Managers. A risk management Standard, Institute of Risk Management (IRM)*, 1. Web: <http://www.e-finance.com> Son Erişim Tarihi: 05.03.2014.
- ARS (Aon Risk Solutions) (2013). *Global Risk Management Survey*, 84. Web: <http://www.aon.com/2013GlobalRisk/2013-Global-Risk-Management-Survey-updated-05-01-2013.pdf> Son Erişim Tarihi: 05.03.2014.
- COSO (2004). *Enterprise Risk Management* Web: http://www.sox-online.com/coso_2004_coso_framework.html.17. Son Erişim Tarihi: 15.01.2014.
- COSO (2014). *Enterprise Risk Management*, Web: <http://www.coso.org/>. Son Erişim Tarihi: 15.01.2014.
- ERM (2004). Enterprise Risk Management— Integrated Framework (ERM) (September, 2004). Executive

summary, 4. Web: http://www.coso.org/documents/coso_erm_executivesummary.pdf Son Erişim Tarihi: 02.01.2014.

FERMA (Avrupa Risk Yönetimi Dernekleri Federasyonu) (2014). *Risk Management*, Web: <http://www.ferma.eu/risk-management/> Son Erişim Tarihi: 12.02.2014.

KGK (Kamu Gözetimi Kurumu) (2014). Riskin Erken Saptanması Sistemi Ve Komitesi Hakkında Denetçi

Raporuna İlişkin Esaslara Yönelik İlke Kararı. Resmî Gazete Sayı: 28945. Web: https://www.kgk.gov.tr/Portalv2Uploads/files/Duyurular/v2/TDS/TDS_2021_Seti/Riskin_Erken_Saptanmasina_Yonelik_Ilke_Karari.pdf Son Erişim Tarihi: 21.03.2022.

WDR (World Development Report) (2014). *Risk management can be a powerful instrument for development*. The World Bank, 61.