

Geleneksel Risk Yönetiminden Kurumsal Risk Yönetim Sistemine Geçiş (*)

Ruveyda KIZILBOĞA (**)

Öz: Yaşanan uluslararası finansal krizlerin ve şirket skandallarının gerisinde yatan nedenlerden birisi de kamu ve özel sektör işletmelerinin risk yönetimi politikalarının yetersiz kaldığı görüşüdür. Bu yetersizliği gidermek ve kurumların daha şeffaf yönetilmesini sağlamak için kurumsal risk yönetim sistemine olan gereksinim artmıştır. Bu çalışmanın amacı, geleneksel risk yönetimiyle karşılaştırmalı olarak kurumsal risk yönetimi sistemini incelemektir. Çalışmada öncelikle geleneksel risk yönetimi sisteminin ortaya çıkışı ve genel özellikleri, kurumsal risk yönetim sisteminin geleneksel risk yönetim sisteminden farklılıkları, kurumsal risk yönetim sisteminin özellikleri ve unsurları, kurumsal risk yönetim sistemine duyulan gereksinim ve bu sistemin önemi ve avantajları üzerinde durulmuştur. Son olarak bu çalışmanın bazı kısıtları olduğu belirtilmiş ve gelecekte bu konuda araştırma yapacaklara bazı öneriler sunulmuştur.

Anahtar Kelimeler: Risk, geleneksel risk yönetimi, kurumsal risk yönetimi, kurumsal risk yönetimi sistemi

Transition from Traditional Risk Management to Enterprise Risk Management System

Abstract: Financial crisis and corporate scandals are thought because of the insufficiency of public and private institutions risk management system. The requirement of enterprise risk management is increased for removing this insufficiency, providing more transparent management systems. The aim of this study is to examine the traditional risk management in comparison with enterprise risk management system. This study first emphasizes the emergence and features the traditional risk management systems, and enterprise risk management differences from traditional risk management system. Then the features and components of enterprise risk management system, the requirement for enterprise risk management and the importance of this system and advantages were emphasized.

Keywords: risk, traditional risk management, enterprise risk management, enterprise risk management system

*) Bu makale "Kurumsal Risk Yönetimi Odaklı İç Denetim ve İstanbul Büyükşehir Belediyesi için Bir Model Önerisi" adlı doktora tezinden üretilmiştir.

**) Dr. Arş. Gör., Nevşehir Üniversitesi
(e-posta: ruveyda.kizilboga@nevsehir.edu.tr)

Giriş

1990'lı yılların sonunda Amerika Birleşik Devletleri başta olmak üzere dünya genelinde yaşanan şirket skandalları, kurumların daha adil ve şeffaf yönetilmesini destekleyen kurumsal yönetim anlayışına ve bu anlayışı destekleyici, kurumun geneline uygulanabilen, kurumsal risk yönetim sistemine ilişkin taleplerin artmasını sağlamıştır. Sistem hem özel sektör işletmelerinin hem de kamu kurumlarının sadece mali alanda risk yönetimi uygulamasından ziyade kurumun tüm alan ve süreçlerinde risk yönetim sisteminin uygulanmasını önermektedir. Bu kapsamda gelecek ve çözüm odaklı bir yönetim anlayışı benimsenmesiyle kaynakların etkili yönetimi sağlanabilir. Bu çerçevede, çalışmanın amacı, geleneksel risk yönetimiyle karşılaştırmalı olarak kurumsal risk yönetimi sistemini incelemektir.

Bu çalışmada kurumsal risk yönetim sisteminin giderek artan önemine dikkat çekilebilmek amacıyla öncelikle risk yönetimi ya da geleneksel risk yönetimi olarak da adlandırılan sistemin ortaya çıkışı ve genel özellikleri incelenmiştir. Kurumsal risk yönetim sisteminin geleneksel risk yönetim sisteminden farklılıkları ortaya konmuş ve kurumsal risk yönetim sisteminin özelliklerine ve unsurlarına değinilmiştir. Son olarak kurumsal risk yönetim sistemine duyulan gereksinim, bu sistemin önemi ve avantajları üzerinde durulmuştur.

1. Risk Yönetim Sistemi ve Gelişim Süreci

Risk yönetim sisteminin ortaya çıkışı ve gelişim sürecini açıklamadan önce risk kavramı ile ilgili bilgi verilmesi kavram karmaşasını ortadan kaldırmak amacıyla faydalı olacaktır. Genel anlamda bir faaliyet ya da olayın sonucuna ilişkin belirsizliği (Terje ve Ortwin, 2010: 8) ifade eden risk kavramının kökeni ile ilgili farklı görüşler bulunmaktadır. Bir görüşe göre risk kavramı İngilizceye, İtalyanca "belirsiz durumlara karşı kadercilikten ziyade bir seçenek oluşturulması" anlamına gelen "risicare" kavramından (Reding, vd., 2009: 4-3); diğer görüşe göre ise onyedinci yüzyıl ortalarında "kayba, zarara veya tehlikeye yol açabilecek bir olayın meydana gelme olasılığı" olarak tanımlanan (Emhan, 2009: 210) Fransızca "risque" kavramından geçmiştir. Onsekizinci yüzyılın ikinci çeyreğinden itibaren İngilizce yazılımı sigortalama işlemlerinde kullanılmaya başlamıştır (Flanagan ve Norman, 1993: 2). Daha çok tehdit edici durumlar için kullanılan risk kavramının "fırsat" olarak kullanılmasına dayanak olarak Çince orjinli bir kelime olması ve Çince'de her iki anlama da sahip olması gösterilmektedir (Derici, Tüysüz ve Sarı, 2007: 152).

Risk çok yönlü bir kavram olması sebebiyle farklı durumlarda farklı şeyler ifade edilmekte ve daha çok algı ve tutumlarla şekillenmektedir (Fone ve Young, 2005: 11-12).

The Committee of Sponsoring Organizations of The Treadway Commission (COSO)'nun tanımına göre risk "bir olayın meydana gelme ve kurumun hedeflerine ulaşma başarısını kötü etkileme olasılığıdır". Basit bir tahminden öte birçok olumsuz sonucu olan önemli bir etmendir (Reding, vd., 2009: 4-3) ve şu anda var olan değil gelecekte ortaya çıkma olasılığı olan tehdit edici durumların genel nitelemesidir (Derici, Tüysüz

ve Sarı, 2007: 152). Tanımda vurgulanması gereken bir unsur da riskin sürekli bir tehdit olma özelliği taşımasıdır (Griffiths, 2005: 17).

İç veya dış kaynaklı bir olay ya da unsur kurumun hedeflerine ulaşma başarısını olumlu ya da olumsuz etkileyebilmektedir (COSO, 2004a: 16). Risk rastlantısal bir olayın meydana gelme olasılığıdır ve gerçekleştiğinde kurumun hedeflerine ulaşma başarısını olumsuz etkilemektedir. Risk üç unsurdan oluşmaktadır. Bunlar: senaryo, meydana gelme olasılığı ve meydana geldiğindeki etki boyutudur (Vose, 2008: 3). Olumlu etkisi olan olaylar, negatif etkileri telafi etmeyi ya da fırsatları temsil etmektedir. Fırsatlar, bir olayın meydana gelmesi durumunda hedeflere ulaşılmasını olumlu etkileme olasılığıdır. Değer yaratan ya da mevcut değeri koruyan (INTOSAI, 2007: 11) fırsatların ortaya çıkması tesadüfî bir durumdur ve hedefler üzerinde olumlu etkisi olmaktadır. Bu nedenle fırsat da aynı risk gibi üç unsurdan oluşmaktadır. Risk ve fırsat bir madalyonun iki yüzü olarak değerlendirilebilir (Vose, 2008: 3).

Her kurumun birbirinden farklı strateji ve hedefleri bulunmaktadır. Riskler strateji oluşturma ve hedef belirleme süreci ile başlamakta (Reding, vd., 2009: 4-3) ve kurumun strateji ya da iş planındaki amaçlara, hedeflere ve riskin olası sonuçlarına dayalı olarak sınıflandırılmaktadır. Risk iç ya da dış kaynaklı ortaya çıkabilen, hedeflere ulaşılmasını engelleyen, kötü yönetime, müşteri-vatandaş memnuniyetsizliğine, ekonomik, mali, varlık ve saygınlık kaybına ve yolsuzluğa sebep olan durumlardır (Managing Risk Across the Public Sector, 2004: 2).

Kısaca risk, plan ve karar sonuçlarındaki belirsizliktir, kaçınılmazdır, stratejik hedeflerin bir fonksiyonudur (Burnaby ve Hass, 2009: 540) ve kurumun başarıya ulaşmasında bariyer rolü üstlenmektedir. İyi şeylerin oluşumunu sağlamak ya da kötü şeylerin oluşumunu engellemek amacıyla risklerin iyi yönetilmesi gerekmektedir (Reding, vd., 2009: 4-3).

Risk yönetimi ise kurumun hedeflerine ulaşmasını engelleyecek risklerin belirlenmesi, azaltılması ve başarıya ulaşılmasını sağlayacak fırsatların ortaya çıkarılarak kullanılması sürecidir (Reding, vd., 2009: 4-3).

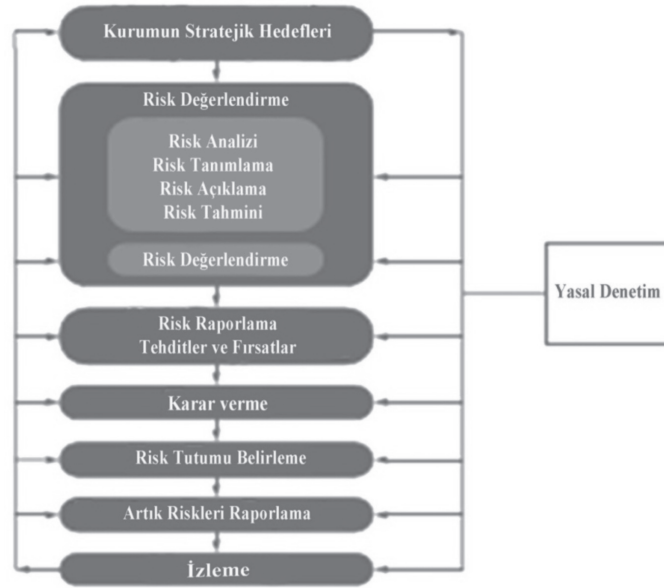
Risk yönetimi kavramı ilk olarak sigortacılık sektöründe kullanılmıştır. 1967'de Londra'da Edward Lloyd tarafından açılan kahve dükkânı zamanla gemicilikle ilgili bilgi alışverişinin yapıldığı bir yer ve kısa süre sonrada denizcilik sigortasının merkezi haline gelmiştir. Risk havuzları oluşturan Lloyd, risklerin kapsamını genişleterek sigortacılık sektörünün lideri konumuna gelmiştir. 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 1973-1979 dönemi petrol krizi sonucunda risk oranlama ve değerlendirme alanında danışmanlık hizmeti talepleri başlamıştır. 1980'lerin ilk yarısı politik risklere ağırlık verilen bir süreçken 1980'lerin sonlarında politik riskler¹ azalmıştır (Non, 8).

1) Berlin Duvarının çöküşü vb. olaylar

1990'da risk yönetimine verilen önem artmış ve daha çok kurumun çökmesine neden olabilecek risklere odaklanılmıştır. 1990 sonlarındaki çalışmalar, kurumların yönetmeleri gereken risk kapsamının genişlediğini ve genişlemeye devam ettiğinin farkına varıldığını göstermektedir. Bütün bunlar risk yönetimine verilen önemin artmasını ve risk yönetim anlayışında kurumsallaşmanın gerçekleşmesini sağlamıştır. Bu dönemde kapsamlı bir risk yönetim çerçevesi oluşturulması, iç denetimin risk yönetim uygulamaları ile bütünleştirilmesi, kurum kültüründe risk farkındalığının ve risk yönetimde yönetim sorumluluğunun artırılması, kurumlarda risk yönetim ofisi oluşturulması ve kurumsal risk yönetim sisteminin kabulü gibi konularda aşama kaydedilmiştir (Non, 10).

Eğer risk yönetimini, riskleri değerlendirmek ve riskin siyasi etkilerini tespit etmek için kullanılan bir yöntem olarak tanımlarsak sistemin uygarlığın başlangıcından beri var olduğunu söyleyebiliriz. Bununla beraber bilinçli bir uygulama olup olmadığı kapsamında değerlendirildiğinde risk yönetiminin 20. yüzyılın ortalarına kadar uzanan bir tarihe sahip olduğu ortaya çıkmaktadır (Non, 7).

Risk yönetimde genelde negatif sonuçlara yoğunlaşıldığı düşünülmekte ve zararı azaltıcı ya da önleyici tedbirler geliştirilmektedir (A Risk Management Standard, 2002: 2). Oysa risk yönetimde her olay ya da projenin hem fırsat sağlayıcı hem de tehdit edici unsurlarıyla aynı anda ilgilenilmektedir. Kurum ve toplumların hedeflerine uygun olarak risklerin incelendiği ve değerlendirildiği resmi bir süreç olan risk yönetimi Şekil 1'de gösterilmektedir.



Şekil 1: Risk Yönetim Süreci

Kaynak: A Risk Management Standard, 2002: 4.

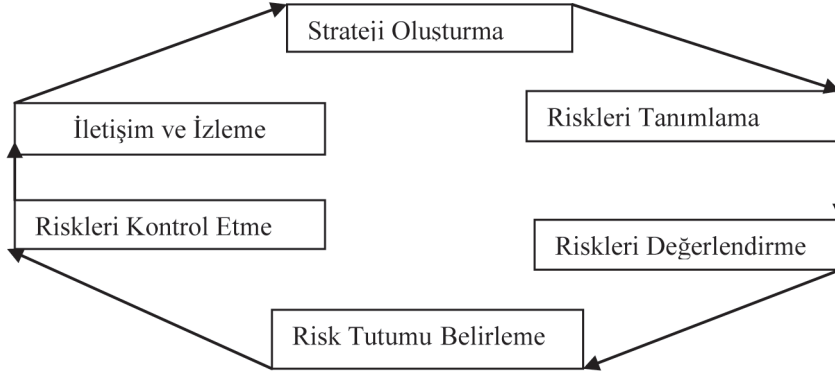
Şekil 1'e göre risk yönetim süreci aşağıdaki aşamalardan oluşmaktadır (Fone ve Young, 2005: 15; Internal Control and Risk Management: A Basic Framework, 2005: 13):

- i. Kurumsal hedefleri anlama.
- ii. Risk yönetim misyonunu tanımlama (hedef ve politika belirleme).
- iii. Risk ve belirsizliklerin değerlendirilmesi (tanımlama, analiz ve ölçme).
- iv. Risk kontrolü (ortadan kaldırma, kaçınma, azaltma, önleme ve yönetim).
- v. Risk finansmanı (riskin finansal sonuçlarının ölçüm değerlendirmesi).
- vi. Program yönetimi (uygulama tedbirleri geliştirme, inceleme ve izleme).

Risk yönetiminin ilk defa uygulanacağı kurumlarda kurumsal yapı sistemin uygulanmasına imkân verecek biçimde şekillendirilmektedir. Bu aşamada sorumlular ve sorumluluklar belirlenmekte, iletişim yapısı uygun hale getirilmekte ve gerekli fiziki donanım sağlanmaktadır (Derici, Tüysüz ve Sarı, 2007: 154). Risklerin yönetimi için kurumun strateji, süreç, personel, teknoloji ve bilgi birikiminin birlikte hareket etmesi gerekmektedir (Walker, Shenkir ve Barton, 2002: 2).

Risk yönetimin amacı gelecekte kuruma zarar verme olasılığı olan olayları ve olayların meydana gelmesi durumunda ortaya çıkacak olumsuz sonuçları azaltmak, olası sonuçlarda meydana gelebilecek sapmaları kontrol etmek, risk yönetim sonuçlarına yönelik farkındalığı artırmak ve hedeflere ulaşılmasını sağlayıcı süreçleri koordine etmektir (Manab, Hussin ve Kassim, 2007: 2; Griffiths, 2005: 21). İyi bir risk yönetim sistemi kurumun; istediği sonuçlara ulaşma güvenini artırır, tehditleri kabul edilebilir bir seviyede etkili bir şekilde tutmasını ve fırsatları kullanarak bilinçli karar almasını sağlar (The Orange Book, 2004: 7).

Risk yönetim fonksiyonunun rolü: risk yönetim strateji ve politikalarını belirlemek; stratejik ve operasyonel düzeyde risk yönetimi sağlamak; risk farkındalık kültürü oluşturmak, buna yönelik eğitimleri koordine etmek; iş birimlerine yönelik risk politika ve yapıları oluşturmak; risk yönetimi için süreçleri tasarlamak ve yeniden gözden geçirmek; kurum içinde risk yönetimini geliştirici faaliyetleri koordine etmek; acil durum ve iş süreklilik programları dâhil olmak üzere risk tutumlarını geliştirmek ve yönetim kurulu ve paydaşlar için rapor hazırlamaktır (A Risk Management Standard, 2002: 11). Risk yönetim sürecinin sürekliliği Şekil 2'de gösterilmektedir.



Şekil 2: Risk Yönetim Sürecinin Sürekliliği

Kaynak: Shenkir ve Walker, 2007: 2.

Risk yönetimi için kapsamlı, uygun ve iyi planlanmış bir stratejiye ihtiyaç vardır (Managing Risk Across the Public Sector, 2004: 3). Risk yönetimi kurum stratejisi ve stratejinin uygulanması kapsamında işleyen ve gelişen sürekli bir süreç olmalı ve kurum kültürüne etkili plan ve programla üst yönetim tarafından entegre edilmelidir. Kurumun dünkü, bugünkü ve özellikle gelecekteki faaliyetleri kapsamında tüm riskler değerlendirilmelidir. Stratejiler uygulama hedeflerine dönüştürülmeli ve kurum yönetici ve çalışanlarının iş alanlarındaki risk yönetim sorumlulukları belirlenmelidir (A Risk Management Standard, 2002: 2). Sorumluların hesap verme sorumluluğu ve performans ölçümü, kurumun her seviyesinde etkinliği artırmak amacıyla, risk yönetim sisteminde desteklenmektedir. Riske yönelik bireysel ya da grup yaklaşımının biçimlenmesinde son edinilen deneyimler ve kurumun ödül veya ceza sistemi etkili olmaktadır (Olson ve Wu, 2010: 3; FERMA, 2003: 10).

Risk yönetimi, kurum hedeflerini destekleyerek kurumu ve paydaşlarını korumakta ve onlara değer katmaktadır (Vicente, 2011: 3). Sistem kurum hedeflerini desteklerken, kurumun gelecekteki faaliyetlerinin tutarlı ve kontrollü bir şekilde oluşumu için bir çerçeve sunar; karar alım süreçlerinin iyileştirilmesine ve kapsamlı ve yapısal iş alanlarının planlanmasına ve önceliklendirilmesine yardımcı olur; sermaye ve kaynakların daha verimli kullanımına ve kurum imaj ve varlıklarının korunması ve geliştirilmesine katkı sağlar; personel ve kurum bilgi tabanını geliştirir ve destekler; kurumun çalışma alanındaki sert kayıp ya da dalgalanmaları azaltır ve kurumsal etkinliği ve verimliliği artırır (A Risk Management Standard, 2002: 4).

Kötü olan risk değil, riskin anlaşılabilmesi, yanlış değerlendirilmesi, yönetilememesi ve göz ardı edilmesidir (Non, 31). İyi bir risk yönetim sistemi ileriye yönelik karar alımında ve yönetiminde kurum yöneticilerine yardımcı olmakta ve sadece kayıpların önlenmesi ya da azaltılması değil, aynı zamanda değer katıcı fırsatların fark edilmesini de sağlamaktadır (Managing Risk Across the Public Sector, 2004: 3).

2. Geleneksel Risk Yönetiminden Kurumsal Risk Yönetim Sistemine Geçiş

Dünya her geçen gün biraz daha risk üstlenerek büyümektedir. Afet, savaş ve finansal çöküşler karşılaşılan birçok riskli duruma verilebilecek örneklerdir. Bir riskin üstesinden geldiğinde arkasından diğeri ortaya çıkmaktadır. Risklerin çeşidi ve miktarı artmakta ve çözüm üretme ihtiyacı bir zorunluluk olarak hem işletme sahiplerinin hem de kamu kurumlarının karşısına çıkmaktadır. Gerekli önlemlerin alınmaması beraberinde felaketleri getirmektedir. Kitlesel ve bazen beklenmedik kurumsal başarısızlıklar, özellikle muhasebe ve raporlamadaki, kurumsal yönetişimde risk yönetimin önemine dikkat çekmektedir (Walker, Shenkir ve Barton, 2002: 2).

İlk risk yönetim uygulaması, kayıpları önlemek için kontrol ve finansman teknikleri ile yönetilmiştir (Manab, Kassim ve Hussin, 2010: 240). Klasik mali yönetim anlayışı olarak tasvir edilen ve geleneksel risk yönetim süreci olarak da bilinen bu sistemde, riskler kötü algılanıp kurum, mal ve finans varlıklarını risklerden korumaya odaklanmakta ve riskleri sözleşme ya da sigortalama yoluyla transfer etmenin yollarını araştırmaktaydı (Road to Implementation ERM for Colleges and Universities, 2009: 9). Sigortalama geleneksel risk yönetim sisteminin en popüler finansal yaklaşımıdır. Sistemde riskler birim birim ya da tek tek yönetilmekteydi. Bu durum yönetim kuruluna ve üst yönetime risklerin genel görünümü ile ilgili bir raporlama yapılamamasına, maliyetlerin artmasına ve risk yönetiminde örtüşmelere neden olmaktadır. Geleneksel risk yöneticileri aynı zamanda paydaşlara değer katma ilkesini de dikkate almamaktaydı (Manab, Kassim ve Hussin, 2010: 240).

Geleneksel risk yönetim sisteminin dar kapsamından çıkarılarak kurumların her türlü faaliyet alanında karşılaşılabilecekleri riskleri (stratejik, faaliyet, uygunluk, raporlama, teknolojik ve personel gibi) ele alabilecek şekilde genişletilmesi gerekmektedir. Gerek özel gerekse kamu sektöründe değişen dünya düzenine uyum çabaları kapsamında kurumsal risk yönetim anlayışı ortaya çıkmıştır.

Kurumsal risk yönetim sisteminin ortaya çıkmasında yeni yönetim anlayışında yer alan “bir işi ilk seferinde doğru yapmak” ve “hata ortaya çıkmadan önlem almak” yaklaşımlarının da etkisi olmuştur. Birbiri ile bağlantılı bu iki yaklaşımdan ilkinin başarı ile uygulanması ikincisinin etkinliğine bağlı kılınmaktadır (Derici, Tüysüz ve Sarı, 2007: 153).

Kurumsal yönetişim anlayışındaki değişim risklerin kurum çapında tanımlanması ve yönetilmesi algısını ortaya çıkarmıştır (Beasley, Jenkins ve Kranitz, 2003: 3). İyi kurumsal yönetişim “kurumun karşı karşıya kaldığı riskleri yönetebilmesi için doğru iç altyapının oluşturulması” anlamına gelmektedir. Kurumsal yönetişim “kurumu hedeflerine ulaşması için bir arada tutan bir tutkal”, risk yönetimi de “esneklik sağlayan bir süreç” olarak değerlendirilmektedir. Aslında kurumsal risk yönetim kavram ve uygulaması “kurumsal yönetişimi güçlendirici önemli bir makine” gibi düşünülmekte ve “kurumsal yönetişimi geliştirmek ve paydaşlara değer katmak temelli” olduğuna inanılmaktadır. Kurumsal yönetişim ve paydaş değeri anlayışının kurumsal risk yönetim anlayışını benimseme ve uygulamada tüzel kişiler için temel motivasyon faktörü olduğu tespit edilmiştir. Kuru-

mun istikrar ve gelişim performansı büyük oranda bu iki unsurun rolünün etkinliğine bağlıdır. Kurumsal yönetim, kurumsal risk yönetim etkinliği için hayati önem taşımakta ve kurumsal risk yönetim unsurları, kurumsal yönetimle uyumlu olmadıkça başarı elde edilememektedir (Manab, Kassim ve Hussin, 2010: 241-242).

Şirket çöküşlerine, skandal ve yolsuzluklara sebep olarak başarısız ya da zayıf risk yönetim ve kurumsal yönetim uygulamaları gösterilmektedir. Örneğin, 1997 yılında ortaya çıkan Doğu Asya mali krizine, zayıf kurumsal yönetim ve yetersiz risk yönetim uygulamaları temel sebep olarak gösterilmektedir (Manab, Kassim ve Hussin, 2010: 242).

Risk yönetiminde sistematik ve bütünsel bir yaklaşım sunan kurumsal risk yönetim sistemi, kurumsal yönetim ve hesap verme sorumluluğunun en temel unsurudur (Terzi, 2010: 1) ve kurumun durumsal farkındalığını artırarak risk tutumlarının daha aktif yönetimini sağlamaktadır (Terzi, 2010: 5). Kurumsal yönetim ve risk yönetiminin birleştirilmesi kurumun; rekabet avantajı kazanmasını ve paydaşlara değer katmasını, bu değeri korumasını ve geliştirmesini sağlamaktadır (Manab, Kassim ve Hussin, 2010: 243-244).

Geleneksel risk yönetim sistemi genel olarak riskin mali yapı üzerindeki olumsuz etkilerinden kurumu korumaya odaklanmakta iken kurumsal risk yönetim sistemi, risk yönetimini kurum stratejisinin bir parçası haline getirmekte ve kuruma değer katmak amacıyla risklere ilişkin en iyi tutumların belirlenmesini ve risklerin etkili yönetilmesini sağlamaktadır (Lienberg ve Hoyt, 2003: 40). Geleneksel risk yönetim ile kurumsal risk yönetim sistemi arasındaki temel farklar Tablo 1’de ele alınmaktadır.

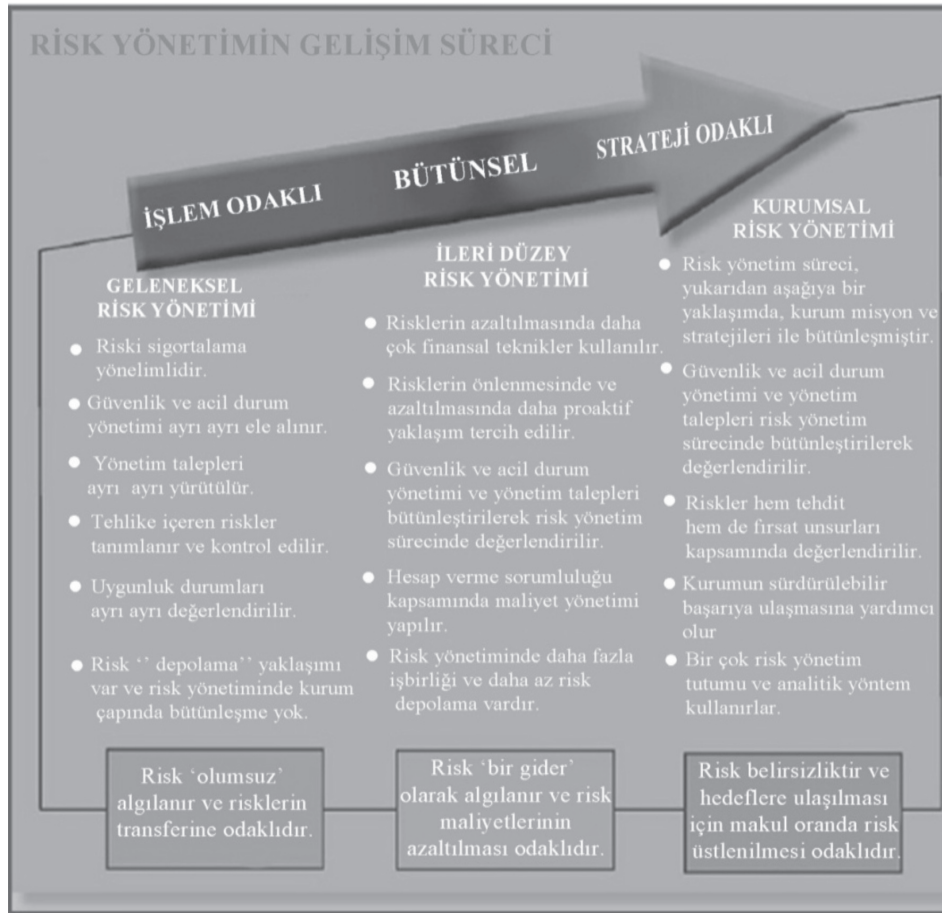
Tablo 1: Geleneksel ve Kurumsal Risk Yönetim Sistemleri Arasındaki Temel Farklılıklar

Geleneksel Risk Yönetimi	Kurumsal Risk Yönetimi
Riskler ayrı ayrı birbirlerinden bağımsız ve diğer faktörlerle bütünleştirilmeden değerlendirilir.	Riskler kurum stratejileri kapsamında değerlendirilir.
Risk tanımlama ve değerlendirmesi söz konusudur.	Risk portföy gelişimi söz konusudur.
Risklerde önem sıralaması yapılmaz.	Riskler önem derecesine göre sıralanır ve buna göre değerlendirilir.
Risk azaltma uygulaması söz konusudur.	Risk optimizasyon uygulaması söz konusudur.
Risk limitleri vardır.	Risk stratejileri vardır.
Risk sahiplenicileri yok.	Risk sorumluları belirlenir.
Rastgele risk ölçümü yapılır.	Risklerin izlenme ve ölçümünde öncelik sıralaması yapılır.
Yapılanmamış ve tutarsız risk yönetim fonksiyonları vardır.	Risk yönetimi kurum genelinde organize edilir ve yürütülür.
“Risk benim sorumluluğum değil” algısı hâkimdir.	“Risk herkesin sorumluluğudur” algısı hâkimdir.

Kaynak: Hall, 2007: 5.

Kurumsal risk yönetim sisteminde üst yönetim ve yönetim risklerin tümüne odaklanmakta ve risklerin kurum çapında etkisini dikkate almaktadır. Böylece geleneksel risk yönetiminden farklılaşmakta ve riskler kurum genelinde değerlendirilmektedir. Ayrıca geleneksel sistemde birim bazında risklere yönelik uygulanan tutumların bir diğer birimde farklı riskler yaratması söz konusu olabilmekteyken (Beasley, Branson ve Hancock 2008: 45-46) kurumsal risk yönetim sistemi ile bu durumun önüne geçilmiştir.

Kurumsal risk yönetim sistemi kurumun bütününe ve tüm risk kategorilerini ele alarak risk yönetim kavramını başka bir seviyeye yükseltmiştir (Terzi, 2010: 5). Bu yükseliş ya da değişim Şekil 3'de gösterilmektedir.



Şekil 3: Risk Yönetimin Gelişim Süreci

Kaynak: Road to Implementation ERM for Colleges and Universities, 2009: 10.

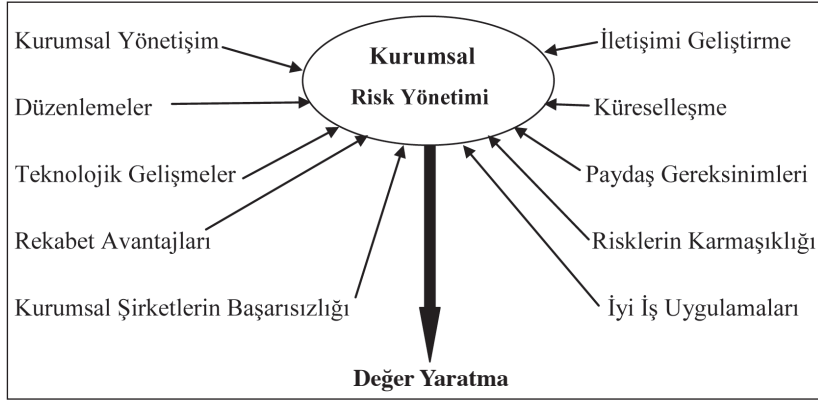
Şekil 3’de görüldüğü gibi işlem odaklı, riskleri kötü algılayan ve yönetmekten ziyade sigortalama yöntemini tercih eden geleneksel risk yönetim sisteminden, risklerin kuruma olan maliyetlerinin azaltılmasına odaklanan ileri düzey risk yönetim sistemine geçilmiştir. Bununla birlikte kurumlar, risklerin yönetilerek avantaja dönüştürülebileceğini savunan kurumsal risk yönetim sistemine yönelmiştir.

3. Kurumsal Risk Yönetim Sisteminin Tanımı ve Özellikleri

Kurumsal risk yönetim sistemi, stratejilerin oluşturulması ve kurum çapında uygulanması, kurumu etkileme olasılığı olan olayların belirlenmesi, risklerin risk iştahı kapsamında yönetilmesi ve kurum hedeflerine ulaşılmasına yönelik makul güvence sağlayan kurum yönetim kurulu, yönetim ve diğer personeli tarafından etki edilen bir süreçtir (COSO, 2004a: 16). COSO’nun tanımı kurumsal risk yönetim sistemi ile ilgili aşağıdaki temel noktaları ortaya koymaktadır (Reding, vd., 2009: 4-4; Woods, 2008: 1077; Beasley, Frigo ve Litman, 2007: 26; Frigo ve Anderson, 2011b: 21):

- i. Kurum çapında sürmekte olan ve her kademedeki çalışanın katkıda bulunduğu akıcı bir süreçtir.
- ii. Kurum stratejisi oluşturulurken uygulanmaktadır.
- iii. Kurumun risk portföy varlık seviyesini oluşturmaya odaklanılmaktadır.
- iv. Meydana gelmesi durumunda kurumu etkileyebilecek olası olaylar belirlenmektedir.
- v. Risklerin kurum risk iştahı kapsamında yönetilmesini sağlayıcı tedbirler alınmaktadır.
- vi. Hedeflere ulaşılabilmesi için bir ya da daha fazla birbirinden ayrı; fakat örtüşen kategorilere yönelinmektedir.
- vii. Kurum üst yönetimine ve yönetime makul bir güvence sağlamaktadır.

Kurumsal risk yönetim yaklaşımı kuruma değer katmak amacıyla strateji, süreç, insan, teknoloji ve bilgi kaynaklarının kurumun karşı karşıya kaldığı belirsizliklerin değerlendirilmesi ve yönetilmesi amacıyla kullanıldığı disiplinli, durağan olmayan, devamlılık ve değişkenlik gösteren kuruma nüfuz etmiş bir sistemdir ve temel sürücüleridir (Manab, Hussin ve Kassim, 2007: 2). Kurumsal risk yönetim sürücülerini Şekil 4’de gösterilmektedir.



Şekil 4: Kurumsal Risk Yönetim Sürücükleri

Kaynak: Manab, Kassim ve Hussin, 2010: 241.

Kurumsal risk yönetim sistemi risklerin entegre edilmesinden daha fazlasını ifade etmektedir. Sistem riski "kurumun hedeflerine ulaşmasını ya da stratejilerini başarıyla uygulamasını olumsuz etkileyen herhangi bir eylem ya da faaliyet olarak" tanımlanmaktadır (Walker, Shenkir ve Barton, 2002: 2). Kurumsal risk yönetim sistemi kapsamındaki temel faaliyetler şunlardır (IIA Position Paper: The Role of Internal Auditing in ERM, 2009: 3; A Practical Guide to Risk Assessment, 14; Maytjewicz, ve D'arcangelo, 5; Tonello, 2007: 10):

- i. Temel misyon ve program hedeflerini düzgün bir şekilde belirlemek ve kuruma bildirmek.
- ii. Kurum risk iştahını belirlemek.
- iii. Risk yönetim çerçevesi dâhil olmak üzere uygun bir iç ortam oluşturmak.
- iv. Kurum hedeflerine ulaşılmasını engelleyici olası tehditleri tanımlamak ve risk evreni oluşturmak.
- v. Etki ve olasılık kapsamında riskleri değerlendirmek.
- vi. Risk tutumlarına karar vermek ve uygulamak.
- vii. Kontrol ve diğer tepki faaliyetlerini yürütmek.
- viii. Kurumun her seviyesinde risklerle ilgili süreklilik temelinde bilgi alışverişi sağlamak.
- ix. Risk yönetim süreci ve çıktılarının merkezi izleme ve koordinasyonunu sağlamak.
- x. Risklerin etkili yönetildiğine dair güvence sunmak.

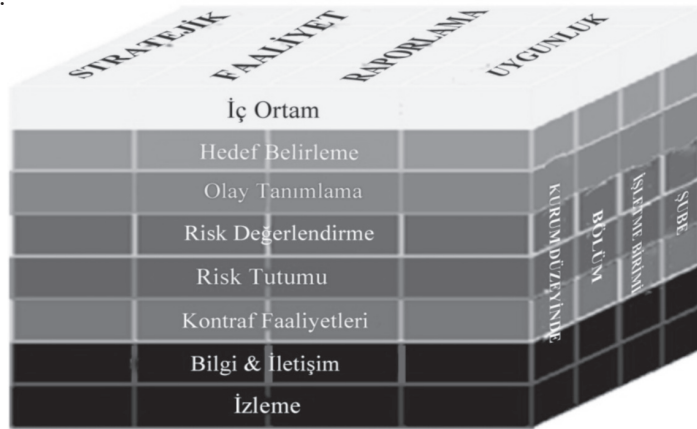
- xi. Bağımsız nesnel güvence ve danışmanlık sağlamak.
- xii. Mevcut sistemlerle (iç kontrol, dış denetim, iç denetim) kurumsal risk yönetim sistemini entegre etmek.

Kurumsal risk yönetimin başlangıç noktası kurum misyon ve vizyonunun belirlenmesidir. Yönetim misyon kapsamında stratejik hedefleri belirler, hedeflere ulaşılmasını sağlayıcı stratejileri seçer (INTOSAI, 2007: 10). Devamında hedeflere ulaşmayı engelleyici riskler ve riskleri azaltıcı kontrol sistemleri ve sorumlular belirlenir. Hedeflere ulaşılmasını etkileyecek olaylar düzenli olarak belirli aralıklarla gözden geçirilir, riskler yeniden değerlendirilir ve gerekli durumlarda yeni risk tutumları saptanır. Performans ve sonuçların zamanında raporlanmasına dikkat edilir (A Practical Guide to Risk Assessment, 14; COSO, 2004a: 39). Bu disiplinli ve sistematik yaklaşım kurumun stratejik, faaliyet, uygunluk, mali vb. risklerini azaltmak amacıyla faaliyetleri planlar, yürütür ve kontrol eder (Razali, Yazid ve Tahir, 2011: 202).

3.1. Kurumsal Risk Yönetim Sisteminin Unsurları

Kurumsal risk yönetim unsurları; “iç ortam, hedef belirleme, olay tanımlama, risk değerlendirme, risk tutumu, kontrol faaliyetleri, bilgi-iletişim ve izleme”dir (Staciokas ve Rupsys, 2005: 23). Unsurlar birbirleri ile ilişkilidir ve hepsi etkili kurumsal risk yönetim sistemini temsil etmektedir (Kinney, 2003: 141).

COSO, kurumsal risk yönetim unsurlarını üç boyutlu küp ile açıklamaktadır (Bkz. Şekil 5). Hedefler dikey olarak, unsurlar da yatay olarak küp üzerinde gösterilmektedir. Kurum ve birimler de üç boyutlu küp üzerinde yer almaktadır. Hedeflerle unsurlar arasında doğrudan bağlantı bulunmaktadır. Unsurlar kurumun ulaşmak için çaba gösterdiği hedeflerin gerçekleştirilmesinde neyin gerekli olduğunu ortaya koymaktadır (COSO 2004a: 23).



Şekil 5: Kurumsal Risk Yönetim Sisteminin Unsurları

Kaynak: Reding, vd., 2009: 4-5.

Şekil 5'de görüldüğü üzere kurumsal risk yönetim sistemi dört hedef ve bununla ilişkili sekiz unsurdan oluşmaktadır. Her unsur her hedefle kesişmektedir. Örneğin, stratejik, faaliyet, raporlama ve uygunluk hedefleri açısından iç kontrol ortamı değerlendirilebilir. Küpün düşey üçüncü boyutunda sekiz unsurun kurumun farklı seviyelerinde (şube, işletme birimi, bölüm ve kurum düzeyine) değerlendirileceği gösterilmektedir.

İç ortam, kurumsal risk yönetimin diğer tüm unsurlarına temel oluşturmakta, disiplin ve altyapı sağlamaktadır. İç ortam unsuru kurumsal strateji ve hedeflerin belirlenmesi, faaliyetlerin yapılandırılması, risklerin tespit edilmesi, değerlendirilmesi ve yönetilmesi süreçlerinde etkili olmaktadır. İç ortam kurumu tümüyle kapsamakta, risk ve kontrollerin kurum personeline nasıl görüldüğüne ve değerlendirildiğine dair bir yaklaşım oluşturmaktadır (COSO, 2004b: 5).

Hedef belirleme, yönetimin misyon ve risk iştahı ile uyumlu kurum hedeflerini belirleme sürecidir (Mattie ve Cassidy, 2008: 4). Hedefler, riskler tanımlanıp uygun tutumlar belirlenmeden önce oluşturulmalı ve kurum risk tolerans seviyesini belirleyen risk iştahı ile uyumlu olmalıdır (INTOSAI, 2007: 22). Hedeflerin belli, anlaşılır, ölçülebilir, ulaşılır, sonuç odaklı ve güncel olmasına özen gösterilmelidir (Burnaby ve Hass, 2009: 545). Hedef belirleme; olay tanımlama, risk değerlendirme ve risk tutumunun belirlenmesinden önceki bir ön koşuldur (Reding, vd., 2009: 4-7).

Olay, stratejilerin uygulanmasını veya hedeflere ulaşılmasını etkileyen iç ya da dış kaynaklı bir oluşum veya hadisedir (COSO, 2004b: 21). Olay tanımlama, kurum hedeflerine ulaşılmasını etkileme olasılığı olan iç ve dış kaynaklı olayların tanımlanması ve sınıflandırılması sürecidir (Mattie ve Cassidy, 2008: 4).

Risk değerlendirme süreci hangi risklerin fırsat ya da gizli bir tehlike içerdiğini tanımlama amaçlı kullanılan kurumsal risk yönetim sisteminin temel bir unsurudur (A Practical Guide to Risk Assessment, 3). Risk değerlendirme kurum hedeflerine ulaşılması ile ilgili risklerin tanımlanması, analiz edilmesi ve uygun tutumların belirlenmesi sürecidir (INTOSAI, 2004: 22):

Risk tutumu ile kast edilen riskler belirlendikten sonra yönetimin risklere yönelik nasıl cevaplar vereceğini (kaçınma, azaltma (kontrol etme), paylaşma ve kabul etme) ya da riskleri nasıl yöneteceğini belirlemesidir (Reding, vd., 2009: 4-7).

Kontrol faaliyetleri, yönetim tarafından belirlenen ve yürütülen risk tutumlarının etkin bir şekilde işlediğine dair garanti veren politika ve prosedürlerdir. Kontrol faaliyetlerinin risk tutumları ile bütünleştirilmiş olması gerekir (Mattie ve Cassidy, 2008: 5).

Bilgi, kurumun her seviyesinde riskleri tanımlamak, değerlendirmek ve tutum belirlemek için gereklidir. Ayrıca kurumu yönetebilmek ve hedeflerine ulaşmasını sağlamak için de gereklidir (COSO, 2004b: 67). İletişim, bilgi sisteminin doğasında mevcuttur. Bilgi sistemlerinin bilgiyi uygun personele taşıması personelin stratejik, faaliyet, raporlama ve uygunluk hedefleriyle ilgili sorumluluklarını sürdürebilmesi için zorunludur (COSO, 2004a: 71).

Kurumlar dinamikdir ve dinamik bir çevrede faaliyet göstermektedir. Bu nedenle hem kurum içi hem de kurum dışı değişiklikler yönetimce değerlendirilmeli yani izleme süreci aktif olarak yapılmalıdır (A Risk Management Standard, 2002: 11).

3.2. Kurumsal Risk Yönetim Sisteminin Önemi ve Faydaları

Sistemin kurulmasıyla kurumun stratejik hedeflerini uygulama yeteneğine doğrudan etki edilmekte ve kurum vizyonuna ulaşılmaktadır (COSO, 2004a: 17). Kurumsal risk yönetimi, süreçlerin gelişimini desteklemekte (IIA Position Paper: The Role of Internal Auditing in ERM, 2009: 2) ve kurumsal yönetişimin önemli bir parçası olduğu dünya çapında pek çok ülke tarafından kabul edilmektedir (Manab, Kassim ve Hussin, 2010: 240). Kurumsal risk yönetim sisteminin etkin işleyebilmesi için cevap aranması gereken temel beş soru bulunmaktadır. Bunlar şu şekilde sıralanabilir (Reding, vd., 2009: 4-10,11):

- i. Neyi başarmak istiyoruz ya da hedeflerimiz neler?
- ii. Hedeflere ulaşmamızı ne engelleyebilir? Risk var mı, var ise ne kadar kötü olabilir ve bu risklerin meydana gelme olasılıkları nedir?
- iii. Risklerin ortaya çıkmasını engellemek için ne yapılabilir? Kurumun risk yönetim stratejisi nedir ve risklere karşı nasıl tutumlar belirlenebilir?
- iv. Kurum riskleri idare etme yeterliliğinde midir? Risk yönetim stratejilerini yürütebilmek için kontrol faaliyetleri tasarlandı mı ve kontrol süreci etkin mi?
- v. İstenen hedeflere ulaşıp ulaşılmadığını test edecek izleme sistemi kuruldu mu?

Kurumlar teknolojinin, yeniden yapılanmanın, pazar değişiminin, rekabetin ve düzenlemelerin yarattığı belirsizlik ortamında faaliyet göstermektedir. Kurumun stratejik tercihleri de belirsizliklerin oluşum kaynağıdır. Örneğin, yeni bir alanda faaliyet yapma yönündeki strateji, beraberinde riskleri ve o alana yönelik fırsatları da getirecektir. Belirsizlikler kuruma değer katıcı fırsatları içerdiği gibi değer azaltıcı riskleri de kapsamaktadır. Önemli olan yönetimin bu belirsizliklerin ne kadarı ile mücadele edebileceğine karar vermesidir. Kurumsal risk yönetim sistemi yönetime, kuruma değer katma kapasitesini artırabilmesi için riskleri ve fırsatları kapsayan belirsizliklerle uygun bir şekilde ilgilenme olanağı sunmaktadır (COSO, 2004a: 13).

Etkili ve disiplinli bir şekilde uygulanan kurumsal risk yönetim sistemi, kurumun işlevsizliğini önleyerek genel riskler yerine önemli risklere yoğunlaşılmasını sağlamakta (Non, 29) ve kuruma rekabet avantajı kazandırmaktadır (Beasley, Branson ve Hancock, 2009: 29; Beasley, Branson ve Hancock, 2011: 4). Ayrıca kurumların yaşamını sürdürme yeteneğini artırarak pozitif bir imaj oluşturmasını sağlamakta, hizmetlerin ve ürünlerin toplam kalitesini olumlu anlamda etkilemektedir (Aksoy, 2005: 188). Kurumsal risk yönetim anlayışının temel unsurlarından biri “ister kâr amaçlı bir şirket ister kâr amacı gütmeyen bir kamu kurumu olsun paydaşlara değer katmak amacı ile var olmak” ilkesidir (COSO, 2004a: 13). Sistem, paydaşlara ve kuruma değer kazandırmak ve bu değeri korumakla kalmaz aynı zamanda bunu geliştirmeye odaklanır (Beasley, Branson ve Hancock, 2008: 45).

Yöneticiler çoğu zaman hedeflere ulaşabilmek adına kurum varlıklarını riske etmektedir (Burnaby ve Hass, 2009: 540); ancak burada amaç, kurum hedeflerine ulaşılmasını engelleyecek belirsizlikleri etkili şekilde yöneterek kuruma değer kazandırmak ve kurumu geliştirmektir (Walker, Shenkir ve Barton, 2002: 2). Bu kapsamda sistemin kuruma sağlayacağı temel faydalar şunlardır (IIA Position Paper: The Role of Internal Auditing in ERM, 2009: 2-3; Terzi, 2010: 5):

- i. Hedeflere ulaşılma olasılığını artırır.
- ii. Yönetimin riskleri anlama, tanımlama ve önlem olarak yönetme yeteneğini geliştirir.
- iii. Birbirinden farklı risk raporlarının yönetim kurulu düzeyinde birleştirilmesini sağlar.
- iv. Önemli riskleri ve onların etki alanlarının anlaşılma düzeyini geliştirir.
- v. Kurum içi çapraz risklerin belirlenmesi ve paylaşılmasını sağlar.
- vi. Ortak ve kesişen riskleri tanımlar ve birimler arası iletişimi güçlendirir.
- vii. Gerçekten önemli konular üzerine odaklanan kaliteli bir yönetim sağlar.
- viii. Kriz gibi ya da başarıyı olumsuz etkileyecek olumsuz durumlarla karşılaşılma olasılığını azaltır.
- ix. İşlerin doğru şekilde yapılmasına odaklanılmasını sağlar.
- x. Başarıya ulaşabilmek için değişiklik yapmaya yönelik inisiyatif alma sorumluluğunu artırır.
- xi. Daha büyük başarılar için daha büyük riskler alma yeteneğini artırır.
- xii. Risk almaya yönelik karar vermede daha bilinçli olunmasını sağlar.
- xiii. Kurumsal verimliliği en uygun hale getirir, korur ve kurumsal imajı güçlendirir.
- xiv. Hesap verebilirliği ve bütünlük iç kontrol sistemini güçlendirir.

Sistem, risk yönetimine verilen önemi artırmakta, yüksek düzeyde sorumluluk alınmasını ve sorumlulukların açıkça belirlenmesini sağlamaktadır (Beasley, Clune ve Hermanson, 2005: 523). Ayrıca standartlar oluşturulmasını ve risklerin daha etkili şekilde yönetilmesi ve azaltılması için fırsat sunmakla birlikte etkinlik ve büyüme için yeni fırsatlar yaratılmasını da sağlamaktadır (Dienhart, 2010: 5). Kurumsal risk yönetim sistemi etkili raporlama, yasa ve düzenlemelere uygunluk ve kayıpların önlenmesi (gelir ya da itibar) konularında da kuruma yardımcı olmaktadır (Florea ve Florea, 2009: 39; Uzun, 2011: 1).

İyi tasarlanmış ve etkin işleyen kurumsal risk yönetim sistemi, yönetim ve yönetim kuruluna kurum hedeflerinin başarılması ile ilgili makul güvence sağlayabilir. Makul güvence, kimsenin kesin tahminlerde bulunamayacağı gelecekteki belirsizlik ve riskleri yansıtmaktadır. Çoğu faktör, bireysel ya da toplu olarak, makul güvence kavramını des-

teklmektedir. Faaliyetler yürütülürken ve sorumluluklar yerine getirilirken hedeflerde başarıya ulaşılması amaçlanır. İyi bir iç kontrol sistemine sahip olan kurumlar, stratejik ve faaliyet hedeflerine yönelik eylemlerden düzenli olarak bilgi sahibi olacaktır. Bununla beraber kontrol edilemeyen bir olay, hata ya da yanlış raporlama meydana gelebilir. Bir başka deyişle, etkin bir kurumsal risk yönetim sistemine rağmen hata ile karşılaşılabilir. Bu nedenle sistemin işleyişinin etkinliği ile ilgili üst yönetime ancak makul bir güvence sunulur ve bu kesin güvence anlamına gelmemektedir (COSO, 2004a: 20).

Güçlü bir kurumsal risk yönetim sisteminin önemi dünya genelinde giderek daha fazla kabul edilmektedir. Kurumlar; sosyal, etik, çevre, finans ve faaliyet alanlarında karşılaştıkları riskleri tanımlamaya ve risklerin kabul edilen seviyede (risk iştahı) yönetimi ile ilgili açıklama yapmaya zorlanmaktadır (IIA Position Paper: The Role of Internal Auditing in ERM, 2009: 2). Risklerin başarılı bir şekilde yönetilmesi için önemli ve stratejik bir çaba gösterilerek kurumsal risk yönetim sorumluluğu kurum çapında üstlenilmelidir (Frigo ve Anderson, 2011a: 1). Ayrıca etkili kurumsal risk yönetimin etik risk yönetimine dayandığı unutulmamalıdır (Demidenko ve McNutt, 2010: 802).

Sonuç

Bu çalışmada geleneksel risk yönetimi sisteminden kurumsal risk yönetimi sistemine geçiş üzerinde durulmaktadır. Kurumsal risk yönetimi, özel sektör uygulamalarıyla başlayan ve yönetim anlayışındaki değişim ile birlikte kamu kurumlarının da dikkatini çeken bir sistemdir. Özellikle küresel ölçekte yaşanan şirket skandalları geleneksel risk yönetim sisteminin yetersizliğinin sorgulanmasına neden olmuş ve sadece mali alanda değil tüm süreçleri kapsayan bir risk yönetim sistemi ihtiyacının ortaya çıkması neticesinde kurumsal risk yönetim sistemi geliştirilmiştir.

Kurumsal risk yönetim sistemi geleneksel risk yönetimindeki gibi riskleri “kötü olumsuz” olarak algılamaz, riskleri yönetilebilir ve kurum için artı bir değere dönüştürülebilir gözüyle değerlendirdiğinden hedeflere yönelik riskler tanımlanarak nasıl tutumlar uygulanabileceği belirlenir ve gözden kaçan fırsatların farkına varılır. Sistem sadece mali tabloların kontrolü ya da uygunluk hedefleriyle değil, tüm faaliyet alanlarıyla ilgili hedeflerle ilgilendiğinden kurumun bütününe hizmet vererek, bütünsellik kazanılmasını sağlar. Kurumsal risk yönetim sistemi kurumun başarısız sonuçlara değil, süreçte başarısız sonuçların ortaya çıkmasına sebep olan nedenlere odaklanılmasını ve onların yönetilmesini ve hatta fırsat sağlayıcı durumların ortaya çıkarılmasını sağlamaktadır. Sonuç itibarıyla, sistemin kuruma sağlayacağı faydalar dikkate alınarak özellikle Türkiye’de kamu kurumlarında uygulanması teşvik edilmelidir.

Bu çalışmanın bazı kısıtları mevcuttur. *Birincisi*, kurumsal risk yönetimi sistemi konusunda Türkçe literatürdeki bilgi eksikliğidir. Bu nedenle çalışmada kurumsal risk yönetimi sistemi konusunda Türkçe’ye kazandırılan terimlerin benimsenmesi için daha fazla çalışmaya gereksinim vardır. *İkincisi*, Türkiye’de özel sektörde ve kamuda kurumsal risk sistemi ile ilgili ölçeklerin henüz geliştirilip uygulanmamış olmasıdır. Bu çalışma ölçek

geliştirilmesi için oluşturulacak zemin açısından teorik çerçeve oluşturmaktadır.

Bu çalışmada geleneksel risk yönetimi sisteminden kurumsal risk yönetimine geçiş üzerinde teorik olarak durulmuştur. Gelecekte araştırma yapacaklara özel sektör işletmelerinde kurumsal risk yönetimine yönelik bir saha araştırması yapmaları önerilebilir. Ayrıca Türkiye'deki özel ve devlet üniversitelerinde kurumsal risk yönetimi ve risk odaklı denetim ilişkisi bir başka inceleme konusu olabilir.

Kaynakça

- Aksoy, T. (2005). Bağımsız Denetim Şirketleri İçin Ulusal ve Uluslararası Düzenlemelerle Uyumlu Çok Yönlü Bir İç Kontrol Anket Formu. Ekim-Kasım-Aralık. S: 73. 168-202.
- A Practical Guide to Risk Assessment, http://www.pwc.com/en_US/us/issues/enterprise-risk-management/assets/risk_assessment_guide.pdf [02.09.2011].
- A Risk Management Standard. (2002). http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf AIRMIC, ALARM, IRM. 1-14. [10.09.2011].
- Beasley, M.S., J.G. Jenkins ve E.F. Kranitz (2003). Implementing ERM: Brainstorming About Risks, Internal Auditing, Internal Auditing. Kasım-Aralık, ABI/INFORM Global. C:18. S: 6. 3-10.
- Beasley, M.S., R. Clune ve D.R. Hermanson (2005). Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation. Journal of Accounting and Public Policy. C: 24. 521-531.
- Beasley, M.S., M.L. Frigo ve J. Litman (2007). Strategic Risk Management: Creating and Protecting Value. Strategic Finance. Mayıs. ABI/INFORM Global. C: 88. S: 11. 24-53.
- Beasley, M. S., B.C. Branson ve B.V. Hancock (2008), Rising Expectations, Journal of Accountancy. Nisan. ABI/INFORM Global. C: 205. S: 4. 44-51.
- Beasley, M.S., B.C. Branson ve B.V. Hancock (2009). ERM: Opportunities For Improvement. Journal of Accountancy. Eylül. C: 208. S: 3. 28-33.
- Beasley, M.S., B.C. Branson ve B.V. Hancock (2011). Developing Key Risk Indicators To Strengthen Enterprise Risk Management. http://www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf [22.02.2011].
- Burnaby, P. ve S. Hass (2009). Ten steps to enterprise-wide risk management. Corporate Governance, C: 9. S: 5. 539-550.
- COSO. (2004a). Enterprise Risk Management-Integrated Framework Executive Summary Framework. Eylül.

- Coso. (2004b). Enterprise Risk Management-Integrated Framework Application Techniques. Eylül.
- Demidenko, E. ve M. Patrick (2010). The Ethics of Enterprise Risk Management As A Key Component of Corporate Governance. International Journal of Social Economics. C: 37. S: 10. 802-815.
- Derici, O., Z. Tüysüz ve A. Sarı (2007). Kurumsal Risk Yönetimi ve Sayıştay Uygulaması. Sayıştay Dergisi, Nisan-Haziran. S: 65. 151-172.
- Dienhart, J. (2010). Enterprise Risk Management: Why The Ethics and Compliance Function Adds Value, 1-23. <http://www.ethics.org/files/u5/ERM.pdf>. [07.08.2011].
- Emhan, A. (2009). Risk Yönetim Süreci ve Risk Yönetimde Kullanılan Teknikler. Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, C: 23. S. 3. 209-220.
- Ferma. (2003). Risk Yönetim Standardı. <http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-turkish-version.pdf>. [11.03.2012].
- Flanagan, R. ve Norman, G. (1993). Risk Management and Construction. Blackwell Scientific.
- Florea, R. ve R. Florea (2009). Internal Audit in Risk Management Approach. Economy Transdisciplinarity Cognition. S: 1. 38-44.
- Fone, M. ve P. C. Young (2005). Managing Risks in Public Organisations. Perpetuity Press.
- Frigo, M. L. ve R. Anderson (2011a). Embracing Enterprise Risk Management Practical Approaches for Getting Started. COSO. http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_001.pdf. [07.08.2011].
- Frigo, M. L. ve R.J. Anderson. (2011b). What is Strategic Risk Management. Strategic Finance. Nisan. 21-22.
- Griffiths, P. (2005). Risk- Based Auditing. Gower Publishing Limited.
- Hall, J. (2007). Internal Auditing and ERM: Fitting in and Adding Value. www.theiia.org/download.cfm?file=66127. [25.06.2011].
- IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management. (2009). The Institute of Internal Auditors. [IIA_PP_Role_of_IA_in_ERM_01.09\[1\].pdf](http://www.theiia.org/documents/IIA_PP_Role_of_IA_in_ERM_01.09[1].pdf). [10.09.2011].
- Internal Control and Risk Management: A Basic Framework (2005). Hong Kong Institute of Certified Public Accountants. http://app1.hkicpa.org.hk/publications/corporategovernanceguides/Guide_Eng_August.pdf. [21.06.2011].
- Intosai. (2004). Guidelines for Internal Control Standards for The Public Sector. 1-

71. <http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf>. [22.05.2011].
- Intosai. (2007). Guidelines for Internal Control Standards for the Public Sector-Further Information on Entity Risk Management. 1-39. [http://www.issai.org/media\(577,1033\)/INTOSAI_GOV_9130_E.pdf](http://www.issai.org/media(577,1033)/INTOSAI_GOV_9130_E.pdf). [22.05.2011].
- Kinney, W. R. (2003). The Research Opportunities in Internal Audit. Auditing Risk Assessment and Risk Management Process. Bölüm 5. Altamonte Springs, FL: The Institute of Internal Auditors.
- Lienberg, A.P. ve R. E. Hoyt (2003). The Determinants of Enterprise Risk Management: Evidence From The Appointment of Chief Risk Officers. Risk Management and Insurance Review, C: 6. S: 1. 37-52.
- Manab, N. A., M.R. Hussin ve I. Kassim (2007). Empirical Study on Theory and Practice of Enterprise-Wide Risk Management (EWRM) on Internal Auditing and Risk Management Functions of Public Listed Companies in Malaysia. http://rmi.nccu.edu.tw/apria/docs/Concurrent%20IV/Session%201/14707EWRM-APRIA_2007_New.doc. [02.05.2011].
- Manab, N. A., M.R. Hussin ve I. Kassim. (2010). Enterprise-wide Risk Management Practices: Between Corporate Governance Compliance and Value Creation. International Review of Business Research Papers. Temmuz. C: 6. S: 2. 239-252.
- Managing Risk Across the Public Sector, (2004) Basan Victorian Auditor-General's Directors: 1-8. http://download.audit.vic.gov.au/files/Managing_risk_report.pdf [Erişim Tarihi: 10.09.2011].
- Mattie, J.A. ve D.L. Cassidy. (2008). Achieving goals, protecting reputation: Enterprise Risk Management for Educational Institutions, <http://www.universityofcalifornia.edu/regents/regmeet/july08/a7a.pdf> [11.09.2011].
- Maytjewicz, G. ve J. D'arcangelo. ERM-Based Auditing. http://www.gapent.com/media/inthenews/Article-Internal_Auditing-ND.pdf. 1-12. [03.11.2010].
- Non, A.J. Are We Ready for Enterprise Wide Risk Management?. 1-37. <http://www.picpa.com.ph/getmedia/114f621e-84bc-45ff-b43a-961532bb55eb/erm.aspx>. [12.09.2011].
- Olson, D.L. ve D. Wu. (2010). Enterprise Risk Management Models, Berlin: Springer –Verlag Berlin Heidelberg.
- Razali, A.R., A.S. Yazid ve I.M. Tahir. (2011). The Determinants of Enterprise Risk Management Practices in Malaysian Public Listed Companies. Journal of Social and Development Sciences. Haziran. C: 1. S: 5. 202-207.

- Reding, F.K., P.J. Sobel, L. U. Anderson, M.J. Head, S. Ramamoorti, M. Salamasick ve C. Riddle. (2009). *Internal Auditing: Assurance&Consulting Services*, 2. Baskı, The IIA Research Foundation.
- Road to Implementation ERM for Colleges and Universities, 2009, Eylül, September. Arthur J. Gallagher Risk Management Services, Inc.
- http://www.ajgrms.com/portal/server.pt/gateway/PTARGS_0_28406_570311_0_0_18/ERM%20TT%20Report%20Final%209-23-09.pdf. [29.05.2011].
- Shenkir, W.G. ve P.L. Walker. (2007). *Enterprise Risk Management: Tools and Techniques for Effective Implementation*. Institute of Management Accountants.1-31. <http://poole.ncsu.edu/erm/document/IMAToolsTechniquesMay07.pdf>. [21.08.2011].
- Staciokas, R. ve R. Rupsys. (2005). *Application of Internal Audit in Enterprise Risk Management*. Engineering Economics. ISSN 1392-2785. S: 2. 20-25.
- Terje, A. ve R. Ortwin. (2010). *Risk Management and Governance*. Springer.
- The Orange Book: Management of Risk-Principles and Concepts*. (2004). October. United Kingdom (UK): HM Treasury.
- Terzi, C. (2010). *Review of Enterprise Risk Management in the United Nations System*, http://www.unjuu.org/data/reports/2010/en2010_4.pdf. [29.05.2011].
- Tonello, M. (2007). *Emerging Governance Practices in Enterprise Risk Management*, The Conference Board, Inc. Research Report R-1398-07-WG, 1-99. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=963221 [01.02.2010].
- Uzun, A. K. (2011). "Kurumsal Risk Yönetimi ve İç Denetim". *Önce Kalite Dergisi*, S. 151. Mart-Nisan. http://www.denetimnet.net/UserFiles/Documents/2011/Kurumsal_Risk_Y%C3%B6netimi_ve_%C4%B0%C3%A7_Denetim.pdf [10.03.2011].
- Vicente, P.F.O. (2011). *A Reference Architecture for Integrated Governance, Risk and Compliance*. <https://dspace.ist.utl.pt/bitstream/2295/1051354/1/dissertacao.pdf> [30.03.2012].
- Vose, D. (2008). *Risk Analysis: A Quantitative Guide*, 3. Baskı. John Wiley&Sons Ltd.
- Walker, P. L., W.G. Shenkir ve T.L. Barton, (2002). *Enterprise Risk Management*. The Institute of Internal Auditors Research Foundation.
- Woods, M. (2008). *Linking Risk Management to Strategic Controls: A Case Study of Tesco Plc*. *International Journal of Risk Assessment and Management*, C: 7. S: 8. 1074-1088.