KURUMSAL RİSK YÖNETİMİNDE UYGULANMASI GEREKEN ADIMLAR*

Arş. Gör. Özlem USMAN**
Prof. Dr. Sait Y. KAYGUSUZ***

Makale Gönderim Tarihi : 07/03/2018 / Kabul Tarihi : 30/10/2018

ÖZ

Bu çalışmada kurumsal risk yönetimi kavramından yola çıkılarak işletmelerin kurumsal risk yönetimini uygulama sürecinde takip etmeleri gereken adımlar ele alınmaktadır. Çalışmanın temel amacı, kurumsal risk yönetim sürecine yönelik yapılan faaliyetler ile ilgili tespitlerde bulunmak ve öneriler sunmak yoluyla işletmelerin mevcut işleyen kurumsal risk yönetim süreçlerine katkıda bulunabilmektir. Bu amaç doğrultusunda işletmelerin risklerini yönetebilmesine yönelik kurumsal risk yönetimi sürecinde izlemesi gereken adımları belirlemek için mevcut literatürde yer alan ve kurumsal risk yönetimi uygulama sürecine değinen çalışmalardan elde edilen bilgiler ışığında sürece yönelik izlenebilecek on bir adımı içeren bir model oluşturulmuştur. Mevcut literatürde yer alan çalışmalar adımların oluşturulmasında genel bir çerçeve olma rolünü üstlenmiştir. Bahsi geçen on bir adım tavsiye niteliği taşımaktadır. Adımların her biri çalışmada alt başlık haline getirilmiş ve adımlarda yürütülmesi gereken faaliyetler de detaylı olarak açıklanmıştır.

Anahtar Kelimeler: Risk Yönetimi, Kurumsal Risk Yönetimi, Kurumsal Risk Yönetim Süreci.

STEPS TO BE APPLIED IN ENTERPRISE RISK MANAGEMENT

ABSTRACT

In this study, the steps to be followed in the implementation process of enterprise risk management are discussed by starting from the concept of enterprise risk management. The main purpose of this study is to contribute to the existing literature about enterprise risk management processes through thoroughly examining the activities previously performed related to the enterprise risk management process and thereby offering suggestions for improving the implementation. To this end, to determine the phases of enterprise risk management implementation, a eleven-step process-oriented model has been developed in the light of the existing studies covering the implementation of enterprise risk management. In order to determine the phases, existing studies in the literature established the general framework. Aforementioned eleven steps are recommended to implement the enterprise risk management process. Each of the steps are subheadlined within the study, and the activities needed to be carried out in the course of designing the steps are explained in detail.

Keywords: Risk Management, Enterprise Risk Management, Enterprise Risk Management Process.

* Bu çalışma Özlem Usman'ın doktora tez çalışmasından üretilmiştir.

** Yalova Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, ozlem.usman@yalova.edu.tr
*** Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi, skaygusuz@uludag.edu.tr

1. GİRİŞ

Günümüzde işletmeler için risk yönetimi denildiğinde artık klasik anlamda kabul edilen risk yönetiminden öte işletmelerin çok farklı kategorilerde ve tüm faaliyet süreçlerinde yer alan riskleri etkin teknikler ile belirledikleri risk iştahları doğrultusunda yönetmeleri, takip etmeleri ve raporlamaları esasına dayalı bir yönetim sistemi olan kurumsal risk yönetimi akla gelmektedir. Bu duruma bağlı olarak kurumsal risk yönetim süreci de işletmeler için kurumsal risk yönetim sisteminin genel çerçevesini meydana getiren unsurları içeren bir süreci ifade etmektedir. Süreç ifadesi, bu yapısı sayesinde işletmelerde kurulacak olan kurumsal risk yönetim sistemi için ana kuralları ve anlayışı gösteren bir rehber özelliğindedir. Bu yaklaşım işletmeler için genel kullanıma uygun olmakla birlikte özellikle belirli bir sektöre hitap etmemektedir. Kurumsal risk yönetim sistemlerinin tasarımları ve uygulanma biçimleri işletmelerin hedeflerine, ihtiyaçlarına, ürün ve hizmet çeşitliliğine, faaliyet süreçlerine ve yöntemlerine göre farklılık gösterecektir (TÜSİAD, 2008: 52).

Çalışmanın konusunu genel olarak kurumsal risk yönetim süreci oluşturmaktadır. Çalışmada öncelikle kurumsal risk yönetimi kavramının ortaya çıkışına değinilerek kurumsal risk yönetim sisteminin içerdiği temel unsurlar açıklanmıştır. Daha sonra kurumsal risk yönetim sisteminin işletmelerde kurulabilmesi ve etkin olarak sürdürülebilmesi için izlenmesi gereken adımları ve adımların her birinde yürütülmesi gereken faaliyetleri içeren kurumsal risk yönetim süreci ele alınmıştır. Mevcut literatürden kurumsal risk yönetim sürecine yer veren farklı çalışmalar incelenmiş ve incelenen çalışmalarda yer alan başlıklar, kurumsal risk yönetimi uygulama sürecinde izlenmesi gereken adımların yer aldığı model önerisine esas teşkil edecek bir çerçeve oluşturulmasında rol oynamıştır. İncelenen çalışmalardan hareketle on bir adımlık bir kurumsal risk yönetim süreci uygulama modeli oluşturulmuştur. Ayrıca adımlar çalışmada başlıklar halinde detaylı olarak açıklanmıştır.

2. KURUMSAL RİSK YÖNETİMİNİN ORTAYA ÇIKIŞI

Kurumsal risk yönetimi, işletme değerini maksimize etmek için kredi riski, piyasa riski, operasyonel risk, ekonomik sermaye ve risk transferini yönetmeye yönelik kapsamlı ve bütünleşik bir çerçevedir (Lam, 2003: 45). Daha geniş bir ifadeyle ise kurumsal risk yönetimi, "İşletme genelinde uygulanan; işletmenin yönetim kurulu, yönetimi ve diğer personelinden etkilenen; işletmenin hedeflerine ulaşmasına ilişkin makul bir güvence sağlamak için işletmeyi etkileyebilecek potansiyel olayları tanımlamak ve belirlenen risk iştahı sınırları içinde yönetmek amacıyla tasarlanmış bir süreçtir. Kurumsal risk yönetiminin yapılan bu tanımı bazı temel unsurları da içerisinde barındırmaktadır. Buna göre kurumsal risk yönetimi (COSO, 2004: 4);

- İşletmede sürekli devamlılık gösteren bir süreçtir.
- İşletmenin her kademesindeki çalışanlar tarafından etkilenmektedir.
- İşletmelerde stratejilerin belirlenmesinde kullanılmaktadır.
- İşletme genelinde her seviyede ve birimde uygulanmaktadır.
- Gerçekleştikleri takdirde işletmeyi etkileyecek potansiyel olayları belirleyebilmek ve riski, risk iştahı doğrultusunda yönetmek için tasarlanmıştır.

- İşletme yönetimine ve yönetim kuruluna makul oranda güvence sağlamaktadır.
- İşletme hedeflerine ulaşılabilmesi için bir araç olma özelliği taşımaktadır.

Kurumsal risk yönetiminin gelişimi büyük ölçüde risk ve risk yönetimi konusuna bakış açısının zaman içinde yaşanan olumsuzlukların da etkisiyle değişmesi ile söz konusu olmuştur (Göğüş, 2015: 15). Kurumsal risk yönetiminin ortaya çıkışı iki ana nedene dayandırılabilir. Bunlardan birincisi, bir dizi yüksek profilli işletme başarısızlığından ve önlenebilir büyük kayıpların ardından işletmelerde kurumsal yönetimin içeriği, alınan riskleri kapsayacak şekilde genişlemiştir. Öyle ki yöneticiler artık işletme içi risk kontrol sistemlerini raporlamaya yüksek derecede ihtiyaç duymaktadırlar. İkinci neden ise, hissedar değeri (shareholder value) modellerinin giderek stratejik planlamada daha büyük bir rol oynamasıdır. Geçmişte stratejik planlama modelleri, riske karşı yetersiz ve zayıf bir dikkat gösterirken günümüzün modern stratejik planlama modelleri, riskin her zaman merkezi bir rol oynadığı finans teorisinden ilham alan hissedar değeri kavramlarına daha fazla dayanmaktadır (Dickinson, 2001: 360).

3. KURUMSAL RİSK YÖNETİM SÜRECİ

Bir işletme geçmişte hiç zarara uğramamış ya da belirgin bir riske maruz kalmamış olabilir. Buna rağmen yönetim kurulu yüksek risklere yol açabilecek olaylar konusunda "kendi işletmelerinde gerçekleşmeyeceği" algısını hiçbir zaman benimsememelidir. Bir işletme sağlam bir stratejiye, yetenekli çalışanlara, düzgün işleyen iş süreçlerine ve güvenilir bir teknolojiye sahip olsa bile diğer her işletme gibi zamanla bazı risklere karşı açık olabilir ve dolayısıyla etkin olarak çalışan bir kurumsal risk yönetim sürecine ihtiyaç duymaktadır (COSO, 2004: 29).

İşletmelerde kurumsal risk yönetimi sürecine göre oluşturulacak uygulama modeli, işletmenin dış çevresi, faaliyette bulunduğu endüstri kolu, faaliyetleri, organizasyonel yapısı, büyüklüğü, teknik alt yapısı, sahip olduğu yönetim ve insan kaynakları politikaları gibi faktörler ile yakından bağlantılıdır. Dolayısıyla her işletme kendi yapısına en uygun modeli oluşturacak ve uygulanan modeller işletmeden işletmeye farklılık gösterir nitelikte olacaktır. Kurumsal risk yönetimini uygulayacak işletmelerin uluslararası örgütler tarafından rehber niteliğinde hazırlanmış olan örnek kurumsal risk yönetim yapılarını kendi işletmelerine uyumlaştırarak kullanmaları sistemin başarısı açısından önemlidir. Bu gerçeklikten hareketle işletmelerin risklerini belirlemek ve yönetmek için uygulayacağı kurumsal risk yönetim sürecinin adımları, konu ile ilgili kaynaklardan detaylı bir şekilde incelenmiştir. Detaylı incelemenin ardından adımlar çeşitli kaynaklardan derlenerek Tablo 1 oluşturulmuştur.

Tablo 1: Kurumsal Risk Yönetim Sürecinin Adımları

	Saka (2008)	Güneş (2009)	Derici (2015)	Arslan (2008)	Ekici (2015)	Günbey* Dönşüm Süreci (2008)	Sarpkaya** Dönşüm Süreci (2012)	Marchetti (2012)	TÜSİAD (2008)	Topçu (2010)	Emhan*** (2009)	Olson ve Wu (2015)	Duran (2013)
Dış Unsurların Belirlenmesi	✓	X	✓	X	X	X	X	X	X	X	X	X	X
İç Unsurların Belirlenmesi	✓	X	✓	X	✓	X	X	✓	X	X	X	X	X
Hedeflerin Belirlenmesi	X	X	✓	X	✓	✓	✓	✓	X	X	X	X	X
KRY Çerçevesinin (Altyapısının) Oluşturulması	✓	X	✓	X	✓	X	X	X	X	✓	X	X	X
Risk İştahının Belirlenmesi	✓	X	✓	X	✓	X	X	✓	X	✓	X	X	X
Risklerin Belirlenmesi	✓	✓	✓	✓	✓	✓	✓	X		✓	✓	✓	✓
Risklerin Analiz Edilmesi ve Ölçülmesi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risklerin Önceliklendirilmesi	✓	✓	✓	✓	X	✓	✓	X	✓	✓	✓	X	X
Risk Yönetimi Strateji Seçimi	✓	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	✓
Bilgi ve İletişim	X	✓	✓	X	✓	✓	✓	✓	✓	X	X	✓	✓
Sürekli İzleme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Yazar adımları "Kurumsal Risk Yönetimi Dönüşüm Süreci" olarak ifade etmiştir.

** Yazar adımları "Kurumsal Risk Yönetimi Dönüşüm Süreci" olarak ifade etmiştir.

*** Yazar, çalışmasında riskleri "Çok önemli, önemli ve önemsiz" olarak sıralamıştır. Bu sıralama tabloda "Risklerin Önceliklendirilmesi" başlığında ele alınmıştır.

Tablo 1 incelendiğinde kurumsal risk yönetim sürecinin ana hatlarının benzer olmasıyla birlikte her kaynakta başlıkların birebir aynı olmadığı görülmektedir. Bu durumun kurumsal risk yönetimi sistemine ait genel kesin bir yapının var olmamasından, işletme yapılarının farklı olmasından ve her araştırmacının kurumsal risk yönetim sürecinin yapısına kendi yorumu ile yaklaşmasından kaynaklandığı söylenebilir. Bu durumla birlikte bazı çalışmalarda (Günbey, 2008; Sarpkaya, 2012) kurumsal risk yönetim sürecinden "dönüşüm süreci" olarak bahsedildiğine de rastlanmıştır. Dönüşüm süreci ifadesi ile kastedilen işletmelerin risklerinin bağımsız olarak görüldüğü ve bu şekilde yönetildiği klasik risk yönetim anlayışından, risklerin tüm işletmede bir bütün şeklinde ele alınarak yönetildiği kurumsal risk yönetimi anlayışına geçiş sürecidir (Günbey, 2008: 94-95). Ancak dönüşüm süreci adımları ile bu çalışmada açıklanacak olan kurumsal risk yönetim sürecinin adımları çoğunlukla benzerlik gösterdiğinden sadece dönüşüm süreci kavramı ile ne ifade edilmek istendiğinden bahsedilmiştir. Esasen dönüşüm süreci adımlarında hedeflerin belirlenmesi, mevcut durumun analiz edilmesi, hedef yapının tespiti, fark analizi ve planlama ile dönüşüm sürecinin uygulanması adımları söz konusudur (TÜSİAD, 2008; Güneş, 2009).

Tablo 1'de yer alan literatür taramasındaki çalışmalara ait detaylar aşağıda açıklanmaktadır.

Saka (2008), kurumsal risk yönetim sürecinin, işletmede öncelikle kurumsal risk yönetim sürecine yönelik ortamın oluşturulması ile başladığını ifade etmektedir. Bu anlamda kurumsal risk yönetim süreci, dış unsurların belirlenmesi, iç unsurların belirlenmesi, kurumsal risk yönetim çerçevesinin oluşturulması, risk alma isteğinin belirlenmesi, risklerin belirlenmesi, risklerin analiz edilmesi ve ölçülmesi, risklerin önceliklendirilmesi, risk yönetim stratejilerinin seçilmesi ve sürekli izleme adımlarından oluşmaktadır.

Güneş (2009), kurumsal risk yönetiminin Türkiye enerji sektöründeki durumuna yönelik yaptığı araştırmada kurumsal risk yönetim sürecini altı başlık altında açıklamıştır. Yapılan çalışmada bu başlıklar, risklerin belirlenmesi ve tanımlanması, risklerin analiz edilmesi ve ölçümü, risklerin değerlendirilerek önceliklendirilmesi, risklere en uygun çözümlerin belirlenmesi, kurumsal risk yönetimi sürecinin sürekli izlenerek gözden geçirilmesi, iletişim ve danışma olarak sıralanmıştır.

Derici (2015), çalışmasında işletmelerde kurumsal risk yönetim sisteminin yapılandırma çalışmaları için uygulayıcılara örnek teşkil edecek bir plan oluşturmuştur. Örnek iş planında kurumsal risk yönetiminin kurgulanma süreci yedi adım olarak gösterilmiştir. Aşamalar sırasıyla iş planı takviminin hazırlanması, kilit personel ile risklerin belirlenmesine yönelik mülakatlar yapılması, misyon, vizyon ve stratejik hedeflerin gözden geçirilmesi, risklerin belirlenmesi, değerlendirilerek karşılanması, kurumsal risk yönetim yapısının belirlenmesi, bilgilendirme ve iletişim, izleme ve kalite güvence olarak belirlenmiştir.

Arslan (2008), çalışmasında kurumsal risk yönetim çalışmalarının yürütülmesinde risklerin tanımlanması, risklerin analiz edilmesi ve ölçülmesi, risklerin önceliklendirilmesi, izleme ve gözden geçirme faaliyetlerinden bahsetmiştir.

Ekici (2015), kurumsal risk yönetim sistemini bir kalkınma ajansında uyguladığı çalışmasında kurumsal risk yönetiminin uygulama faaliyetlerini sekiz başlık altında ele almıştır. Söz konusu başlıklar iç ortamın iyileştirilmesi faaliyetleri, hedeflerin belirlenmesi, risklerin tanımlanması, risklerin değerlendirilmesi, risklere yönelik tepkilerin ve kontrol faaliyetlerinin belirlenmesi, bilgi ve iletişim faaliyetleri, izleme faaliyetleri ve risk kütüğünün oluşturulması faaliyetleri olarak sıralanmıştır.

Günbey (2008), kurumsal risk yönetiminde iç denetimin rolünü incelediği çalışmasında kurumsal risk yönetimi sürecini dönüşüm süreci olarak ifade etmiş ve kurumsal risk yönetimi dönüşüm sürecini sekiz aşamada açıklamıştır. Çalışmada bu aşamalar sırasıyla hedeflerin belirlenmesi, risklerin tanımlanması, risklerin analizi ve ölçülmesi, risklerin önceliklendirilmesi, risk transferi, risk yönetim eğitimi, sürecin sürekli izlenerek gözden geçirilmesi, iletişim ve danışma olarak belirlenmiştir.

Sarpkaya (2012), da çalışmasında kurumsal risk yönetiminde iç denetimin rolünü incelemiş ve kurumsal risk yönetimi sürecini dönüşüm süreci olarak ifade ederek süreci sekiz başlık halinde açıklamıştır. Bu başlıklar hedeflerin belirlenmesi, risklerin tanımlanması, risklerin tahlili ve ölçümü, risklerin önceliklendirilmesi, risk transferi, risk yönetim eğitimi, sürecin sürekli izlenerek gözden geçirilmesi, iletişim ve danışma olarak sıralanmıştır.

Marchetti (2012), kurumsal risk yönetim sürecini sekiz adım olarak ele almıştır. Söz konusu adımları, iç çevrenin belirlenmesi, strateji ve hedeflerin belirlenmesi, olay tanımlama, risk değerlendirme, risklere cevap verme, iletişim, izleme ve gözden geçirme olarak sıralamış ve her bir adımı detaylı şekilde açıklamıştır.

TÜSİAD (2008), risk yönetimi çalışma grubu tarafından hazırlanan kurumsal risk yönetimi raporunda kurumsal risk yönetim sürecinin temel unsurlarını risklerin tanımlanması, risklerin analiz edilmesi ve ölçülmesi, risklerin önceliklendirilmesi, risklere uygun çözümlerin belirlenmesi, sürecin sürekli izlenmesi ve gözden geçirilmesi, iletişim ve danışma olarak altı başlık altında açıklamıştır.

Topçu (2010), finans dışı şirketlerde kurumsal risk yönetimi konusunu temel alarak hazırladığı çalışmasında kurumsal risk yönetimi modelini altı aşama olarak ifade etmiştir. Bu aşamalar, kurumsal risk yönetimi altyapısının tesis edilmesi aşaması, risklerin tanımlanarak sınıflandırılması aşaması, risklerin önceliklendirilmesi aşaması, risklerin ölçümü aşaması, risk kontrol faaliyetlerinin geliştirilmesi aşaması ve raporlama aşaması olarak sıralanmıştır.

Emhan (2009), risk yönetim süreçlerini inceleme konusu olarak ele aldığı çalışmasında risk yönetim sürecinin aşamalarını riskin tanımlanması, riskin değerlendirilerek hesaplanması, alternatif olan risk düzeltme araçları içinden seçim yapmak, seçilen risk düzeltme araçlarının uygulanması ve sonuçların kontrolü olarak beş başlık altında toplamıştır.

Olson ve Wu (2015:7) ise kurumsal risk yönetim sürecinden bahsederken risklerin belirlenmesi, analiz edilmesi, risk tutumlarının belirlenmesi, sürekli izleme ve raporlama adımlarına ek olarak "kontrollerin belirlenmesi" adımına da yer vermiştir. Kontrollerin belirlenmesi aşaması daha çok risklerin etkili bir şekilde ele alındığı ve en uygun ve etkin tutumunun saptanması için yapılması gereken kontrollerin belirlendiği aşama olarak ifade edilmiştir.

Duran (2013), hazırladığı araştırma raporunda risk yönetim sürecinin, stratejik plan çalışmaları ile eş zamanlı şekilde başlatılması gerektiğinden bahsetmiş ve risk yönetimi sürecinin aşamalarını risklerin tespit edilmesi, risklerin değerlendirilmesi, risklere cevap verilmesi, risklerin gözden geçirilmesi, iletişim ve raporlama olarak beş aşamada sıralamıştır.

Kurumsal risk yönetim süreci ile aşağıda yer alan beş temel soruya doğru ve etkin yanıtların alınmasına fayda sağlamak amaçlanmaktadır. Bu sorular şunlardır (TÜSİAD, 2008: 52):

- İşletmede risklerin neler olduğu gerçekten biliniyor mu?
- Bu riskleri etkin bir şekilde yöneterek, risk / kazanç dengesi lehde kullanılabiliyor mu?
- Riskler için uygun kontroller var mı?
- Kontroller etkili bir biçimde çalışıyor mu?
- Hangi kontroller iyileştirilmek / geliştirilmek zorundadır?

Mevcut literatürden incelenen farklı kaynaklar bu çalışmada kurumsal risk yönetimi uygulama sürecinde izlenmesi gereken adımların yer aldığı model önerisine esas teşkil edecek bir çerçeve oluşturulmasında rol oynamıştır. İncelenen kaynaklarda yer alan kurumsal risk yönetim süreç adımlarının birbirilerinden farklı olmasıyla birlikte esas itibariyle ana prensiplerin benzer olduğundan bahsetmek mümkündür. Bu gerçeklikten yola çıkılarak bu çalışmada, mevcut literatürdeki çeşitli kaynaklardan derlenen ve Tablo 1'de toplu şekilde özet halinde gösterilen on bir adımlık bir kurumsal risk yönetimi uygulama süreci oluşturulmuştur. Her bir adım alt başlık haline getirilerek adımların ne ifade ettiği ve söz konusu adımlarda yürütülmesi gereken faaliyetler detaylı olarak açıklanmıştır.

3.1. Dış Unsurların Belirlenmesi

İşletmenin faaliyette bulunduğu politik, kültürel, finansal ve sosyal çevre ile rekabet çevresi ve bunlara ilave olarak kritik iş unsurları ile dış paydaşlar işletme için dış unsurları oluşturmaktadır. Dış unsurların belirlenmesi, işletmenin çevresinde yer alan fırsat ve tehditleri belirlemesi bakımından önem taşımaktadır (Saka, 2008). Böylelikle dış unsurlardan gelebilecek riskler de önceden tahmin edilebilecektir. Dış unsurların kapsamında, parlamento, sivil toplum kuruluşları, üniversiteler, medya uluslararası taahhütler, ekonomik ve siyasi dalgalanmalar gibi yönetimin önemli olduğuna inandığı ve işletme faaliyetlerini etkileyen tüm ilişkiler sayılabilmektedir (Derici, 2015: 35).

Yürütülen kurumsal risk yönetim sisteminin işletmede çoğunlukla işletmenin kontrolü dışında gerçekleşen ve dış unsurlardan kaynaklanan durum ya da olayları kesin olarak engellemesi söz konusu değildir. Ancak etkin işleyen bir kurumsal risk yönetim sistemi dış unsur kaynaklı durumlar karşısında işletmede yönetim cephesinde daha sağlıklı ve isabetli kararlar alınabilme ihtimalini arttırabilir. Bu nedenle kurumsal risk yönetim sürecinin ilk adımlarında dış unsurların belirlenmesi başarı için önemlidir.

3.2. İç Unsurların Belirlenmesi

Kurumsal risk yönetim sisteminin işletmelerde kurulabilmesi için işletmenin faaliyet türü, faaliyet alanı, etik değerleri, insan kaynakları politikaları, organizasyonel yapısı, yönetim anlayışı gibi konular hakkında geniş bilgiye sahip olunması gereklidir. İşletmenin iç ortamının tespiti yönetimin tutum ve davranışlarının anlaşılmasını sağlar. Kurum her yönüyle kendisini tanımalıdır (Kızılboğa, 2013: 204). İşletmenin her yönüyle kendisini tanıması güçlü ve zayıf yönlerinin farkında olarak güçlü yönlerini korumaya zayıf yönlerini ise geliştirmeye çalışması açısından önem taşımaktadır.

İç unsurlar, kurumsal risk yönetim sisteminin kurgulanması için bir temel oluşturmaktadır. Bu alandaki unsurlar bir işletmenin risk yönetimiyle ilgili tarzına da yön vermektedir. İşletme içi unsurlar; işletmelerde hazırlanan iş planı yapısını, hedef belirleme ve risklerin belirlenerek değerlendirilme sürecini etkiler. Aynı zamanda kontrol faaliyetlerinin tasarımı ve uygulanması ile kurum içi iletişim ve izleme faaliyetleriyle de yakından ilgilidir (Marchetti, 2012: 32).

Kurumsal risk yönetiminin uygulanması sürecinde işletmede faaliyette bulunan tüm çalışanların işletmenin vizyonu ve misyonu hakkında bilgi sahibi olması ve içselleştirmesi önemlidir. Bunun yanı sıra hali hazırda yürütülmekte olan risk yönetim sisteminin durumunun incelenmesi de sürece yönelik atılacak adımlarda yol gösterici olacaktır.

3.2.1. Vizyon ve Misyon Hakkında Bilgi Sahibi Olma

Vizyon en geniş ifade ile "*geleceğin resmi*"dir. Vizyon bir işletmenin değerlerinin ve amaçlarının en temel ifadesi olarak kabul edilmektedir ve işlemenin geleceği için bir yol haritası sunmalıdır (Kılıç, 2010: 89). Misyon ise en genel ifade ile işletmenin "*var oluş amacı*"dır. Misyon kavramı işletmenin şu anda neden var olduğunu belirtir (Kılıç, 2010: 91).

İşletme kendisini tanımasının ardından vizyon ve misyonunu belirlemelidir. Eğer bunlar belirlenmemiş ya da yanlış ve eksik bir şekilde belirlenmiş ise gereken düzeltmeler yapılmalıdır. Vizyon ve misyon işletme için kurumsal kimliğinin meydana gelmesinde somut adımlardır. Vizyon ve misyonun belirlenerek tüm çalışanlar tarafından bilinmesi ve benimsenmesi gereklidir. Vizyon ve misyonun işletmede belirlenmesi kurumsal risk yönetim sisteminin kuruma yerleştirilmesini de kolaylaştırıcı bir rol oynamaktadır (Kızılboğa, 2013: 204).

3.2.2. Mevcut Risk Yönetim Sisteminin Durumunun İncelenmesi (Durum Analizi)

İşletmenin mevcut durumdaki risk yönetim alt yapısını detaylı olarak analiz etmesi, karşı karşıya kaldığı risklere yönelik oluşturduğu sistemi ve sistemin performansını anlayabilmek için önemlidir. Mevcut durum analizi hali hazırda işletmenin karşılamak durumunda kaldığı risklere yönelik nasıl bir durumda olduğunu ifade eder. (Arslan, 2008: 53). Mevcut sistemde risk yönetim sürecinde kullanılan araçlar, yapılan uygulamalar incelenmeli, sürecin söz konusu olan kuvvetli ve zayıf yönleri belirlenmelidir (Günbey, 2008: 98).

İşletmede kurumsal risk yönetim sistemi bulunmayıp yalnızca bir birim ya da bölümde dahi risk yönetim sistemi uygulanıyorsa bile buradan sağlanacak veriler analiz edilmelidir. Diğer yandan yürütülen bir risk yönetim sistemi var ise mevcut durumun incelenerek eksikliklerin tespit edilmesi, sağlıklı bir kurumsal risk yönetim sisteminin işletmeye yerleştirilmesi açısından önem taşımaktadır.

3.3. Hedeflerin Belirlenmesi

Hedeflerin belirlenmesi adımı, kurumsal risk yönetimi perspektifinden bakıldığında genel işletme stratejileri ve kurumsal risk alma profili olmak üzere iki başlık altında incelenmelidir. İşletmelerin öncelikle mevcut konumlarını, hedeflerini ve bu hedeflerine ulaşabilmek için neler yapması gerektiğini tanımla-

yan bir işletme stratejisi ve politikası olmak zorundadır. İşletme stratejisinin bilinmediği bir durumda, işletmede kurumsal risk alma profilinin uygunluğundan bahsetmek ve bu profili değerlendirmek söz konusu olamamaktadır. İşletme stratejileri ve kurumsal risk alma profilleri birbirleri ile uyumlu birbirlerinden etkilenen ancak birinin diğerinin bir sonucu olarak algılanmaması gereken kavramlardır Bu iki kavramı net olarak bilinmesi işletme için önemlidir. Zira bir işletmenin hedefleri ve belirlenen stratejilerinin varlığı, işletmenin hissedar değeri oluşturma ve risk yönetimi uygulamalarına zemin olacak iş modelinin belirlenmesine katkıda bulunacaktır (TÜSİAD, 2008: 34).

Kurumsal risk yönetimi sisteminin işletmede yürütülmesi sayesinde başarılması istenen hedefler ortaya konmalıdır (Kızılboğa, 2013: 209). COSO'nun kurumsal risk yönetimi modelini oluşturan bileşenlerinde hedefler dört kategoride sınıflandırılmaktadır. Bunlar; işletmenin üst düzey hedeflerini oluşturan stratejik hedefler, işletme kaynaklarının etkin ve verimli kullanımı ile ilgili tüm faaliyetleri kapsayan operasyonel hedefler, yönetimin karar alma ile işletme faaliyet ve performansını izleme süreçlerini destekleyen yönetimin amacına uygun gereken bilgileri doğru ve eksiksiz şekilde sağlamasına destek olan güvenilir raporlama hedefleri ve yürürlükteki kanun ve yönetmelikler ile işletmenin içinde bulunduğu pazar şartları, fiyatlandırma politikaları, vergilendirme, çevrenin korunması, çalışan refah düzeyi ya da uluslararası ticaret kuralları ile ilgili olabilecek düzenlemelere uygun faaliyette bulunmaya yönelik olan uygunluk hedefleridir (COSO, 2004: 37). İşletme hedeflerinin bu şekilde sınıflandırılması kurumsal risk yönetiminin farklı açılardan ele alınabilmesine imkân sağlar (Ekici, 2015: 92-93). Stratejik, operasyonel, raporlama ve mevzuata uygunluk olmak üzere dört kategoriye ayrılan işletme hedefleri belirlendikten sonra söz konusu hedeflere ulaşabilmek için işletmede yapılacak faaliyetler ve alınacak kararlar belirli aralıklarla kontrol edilmelidir. Burada önemli olan nokta özellikle stratejik ve operasyonel hedefler konusunda olmaktadır. Çünkü işletmenin belirlediği stratejik ve operasyonel hedeflere ulaşılması durumu her zaman tamamıyla işletmenin kontrolünde olmamaktadır. Kurumsal risk yönetimi bu hususta işletme yönetimine işletmenin, belirlemiş olduğu hedeflerinin neresinde bulunduğu ile ilgili olarak zamanında ve doğru bilgi sağlayacağına dair makul bir oranda güvence vermektedir (Günbey, 2008: 97).

İşletmede kurumsal risk yönetim sisteminin tasarımını ve geliştirilmesini kolaylaştırmak için açıkça belgelenmiş bir strateji ve ilgili hedefler gereklidir. Bu bilgi ve rehberliklerin olmaması önerilen kurumsal risk yönetim sistemini geliştirme prosedürünü takip etmeyi imkansız hale getirmektedir. Dolayısıyla, bu adım süreç için çok önemlidir. Hedeflerin oluşturulması, kurumsal risk yönetiminde risk belirleme, risk analizi ve risk yönetimiyle devam eden müteakip sistem aşamaları için bir ön şart niteliğindedir. Yönetim, işletmede stratejik hedefleri belirler. Strateji ve operasyonları, raporlamayı ve uygunluk hedeflerini tanımlar. Stratejik hedefler, işletmenin misyonunu ve amaçlarını destekleyen hedeflerdir. Bu hedefler çalışanlara sunulmalı, anlaşılabilir ve ölçülebilir olmalıdır. Çalışanlar işletmenin hedefleri ile rolleri ve sorumlulukları arasındaki ilişkiden haberdar olmalıdır (Marchetti, 2012: 36-37). Ayrıca hedeflerin belirlenmesi sürecinde işletme stratejileri- risk iştahı ve bunların işletme vizyonu ve misyonu ile olan ilişkileri de dikkate alınmalıdır. İşletmenin alt bölümleri için geçerli olan hedefler, işletmenin stratejik hedefleriyle bütünleşik şekilde belirlenmeli ve dökümante edilmelidir (Ekici, 2015: 93). Örneğin hedef kategorilerinden biri olan güvenilir raporlama sayesinde işletmenin hedefleri ile mevcut durumu arasındaki bağlantı sağlıklı bir şekilde öğrenilerek gerekli düzeltmelerin yapılması sağlanabilmektedir.

3.4. Kurumsal Risk Yönetim Çerçevesinin Oluşturulması

Kurumsal risk yönetim süreci farklı görev ve sorumluluklara sahip olan birçok farklı kişi tarafından yürütülür. Yönetim kurulu (gerek doğrudan gerekse diğer komiteler aracılığı ile), yöneticiler, iç denetçiler ve diğer birim çalışanları süreçte yer almaktadırlar (Yılmaz, 2007: 131). Kurumsal risk yönetim sisteminin işletmede yürütülmesinde çalışanların sistem kapsamındaki rol ve sorumluluklarının, yetkilerinin belirlenebilmesi amacıyla kurumsal risk yönetimi organizasyon yapısının oluşturulması ve dokümante edilmesi gereklidir (Ekici, 2015: 152). Organizasyon yapısında yönetim kurulunun, kurumsal risk yönetim komitesinin, risk yöneticilerinin ve finansal yöneticilerin, iç ve dış denetçilerin görev ve sorumlulukları belirlenmiş olmalı, ayrıca tüm çalışanların üstlenmesi gereken roller işletme yönetimi tarafından detaylı olarak çalışanlara aktarılmış olmalıdır.

İşletme üst yönetiminin farkındalığı, risk yönetimine olan inancı ve desteği olmaz ise risk yönetiminin işletme içerisinde benimsenmesinden ve başarısından bahsetmek mümkün değildir. Buna ilave olarak yönetim kurulunun talep etmesi ve üst yönetimin desteği ile yürütülecek olan risk yönetim faaliyetlerinin işletme içerisinde mutlaka bir sorumlusu da bulunmalıdır. Sorumluluk, risk yönetim faaliyetlerinin daha sistematik ve planlı ilerlemesini sağlamaktadır. Risk yönetim faaliyetlerinin koordinasyonu için işletmede bir birim görevlendirilmelidir. Bu birim, ayrı bir risk yönetim departmanı şeklinde kurulabileceği gibi kalite birimi, stratejik yönetim ya da planlamadan sorumlu olan bir birim de olabilir. Birimin sorumluluk alanları belirlenerek, faaliyetlerini etkili bir şekilde yürütebilmesi için gereken insan kaynağı ve mali destek de sağlanmış olmalıdır. Kurumsal risk yönetim faaliyetlerinin koordinasyonundan söz konusu birimin sorumlu olduğu yazılı düzenlemelerde de yer almalı ve tüm işletme çalışanları da bu konuda haberdar edilmelidir (Kaya, 2015: 326-327). Her ne kadar işletme içerisinde bazı birimler kurumsal risk yönetim süreci ile daha yakından ilgili olduklarından daha fazla rol ve sorumluluğa sahip olsalar da genel itibariyle işletme içerisinde çalışan her birey bu sürece bir şekilde katkıda bulunmaktadır. Bu açıdan bakıldığında sürecin sağlıklı işlemesinde tüm çalışanların sorumluluk sahibi olması gerektiği de düşünülmektedir.

Bazı işletmelerde risk yönetim sorumluluğunda yalnızca bir kişi bulunurken, bazı işletmeler büyük bir ekip çalıştırmaktadır. Her iki yaklaşımın da farklı avantajları söz konusudur. Büyük bir ekipte, daha fazla kaynak ve çalışan yapılacak olan risk yönetim faaliyetlerine odaklanmaktadır. Bununla birlikte, daha küçük bir kurumsal risk yönetim ekibi, iş birimlerini, yönetimi ve çalışanları daha yüksek düzeyde özveride bulunmaya, risk yönetim faaliyetlerine katılma konusunda ve faaliyetler hakkında bilgi paylaşımında daha fazla sorumluluk almaya ve risk yönetim faaliyetlerini daha çok sahiplenmeye teşvik edebilmektedir. Bu anlamda kurumsal risk yönetim altyapısını oluştururken genel yaklaşım, yapılacak risk atölyelerini kolaylaştırmak, yöneticilerin ve iş birimlerinin riskleri anlamasına yardımcı olmak, işletme genelinde gerekli verileri toplamak ve riskleri üst düzey yöneticilere ve yönetim kuruluna raporlamaya yardımcı olmak için kurumsal risk yönetimi ekibinde makul bir sayıda çalışanın görevlendirilmesi yönündedir. Uygulamada işletmelerde kurumsal risk yönetimin altyapısına yönelik birçok yaklaşım bulunsa da, yapı oluşturulurken yaygın olarak kullanılan ortak öğeler aşağıdaki gibi sıralanabilir (IMA, 2007: 23).

- CEO'nun taahhütlerini (üst yönetimden gelen mesajları) göz önde bulundurmak,

- Herhangi bir işletme riskini veya denetim komitesi tüzüğünü kurumsal risk yönetimini dâhil etmek için uyarlamak da dâhil olmak üzere, risk politikaları ya da görev bildirimleri hazırlamak,
- İş birimlerine, yöneticilere ve yönetim kuruluna raporlama yapmak,
- İşletmede kurumsal risk çerçevesinin benimsenmesi veya geliştirilmesi,
- Ortak bir risk dilinin benimsenmesi veya geliştirilmesi,
- Risk tanımlama tekniklerini kullanmak,
- Riskleri değerlendirme araçlarını kullanmak,
- Riskleri raporlama ve izleme araçlarını kullanmak,
- Çalışanların görev tanımlarına ve sorumluluklarına uygun olan riskleri, çalışanlar ile birlikte değerlendirmek,
- Riskleri işletmede bütçeleme fonksiyonları içerisine dâhil etmek
- Kurumsal risk yönetim sistemini işletme stratejisine entegre etmek.

Kurumsal risk yönetim altyapısının kurulması, kurumsal risk yönetim sürecinde yer alan adımların sağlıklı olarak yürütülmesi yönünde bir temel teşkil etmektedir. Kurumsal risk yönetimi uygulamasına karar verilen bir işletmede organizasyonel anlamda yapılması gereken hazırlıkların da tamamlanmış olması beklenmektedir. Çalışanların görev ve sorumluluklarının belirlenerek hayata geçirilmesinin sistem başarısı için önemli bir unsur olduğu unutulmamalıdır (Topçu, 2010: 58).

3.5. Risk İştahının Belirlenmesi

Risk iştahı, bir işletmenin değer yaratma arayışındayken kabul etmeye istekli olduğu risk miktarıdır. Her işletme kendi içinde değer yaratabilmek için çeşitli hedefler belirlemektedir ve bunu yaparken üstlenmeyi düşündüğü riskleri de geniş ölçüde anlamalıdır. COSO, risk iştahını belirlemek için üç adım önermektedir (Olson ve Wu, 2015: 6):

1. Risk iştahının geliştirilmesi adımı, bu adım işletmenin karşı karşıya bulunduğu risklerin mevcut seviyesinin ve dağılımının, işletmenin üstesinden gelebileceği risk düzeyinin değerlendirilmesi, işletmenin kabul edilebilir risk seviyesi, büyüme, risk ve risklerin geri dönüşü konusundaki tutumlarının göz önünde bulundurulmasını gerektirir.
2. İşletmeye uygun olan risk iştahının kararlaştırılmasının ardından gelen adım, işletme genelinde tüm çalışanların konu hakkında bilgi sahibi olmasının sağlandığı adım olmalıdır.
3. İşletmeyi etkileyen risklerin, nicel ve nitel ölçütler açısından izlenmesi de risk iştahının belirlenmesi için son adımı oluşturmaktadır.

Risk iştahı, işletme tarafından belirlenecek olan subjektif bir kavramdır. İşletmede belirlenen düşük risk iştahı yüksek riskten korunma oranını, yüksek risk iştahı ise düşük riskten korunma oranını ifade etmektedir (Topçu, 2010: 81).

3.6. Risklerin Belirlenmesi

İşletmelerin, risklerini yönetebilmek için hangi risklerle karşı karşıya olduklarını bilmeleri ve söz konusu riskleri değerlendirmeleri gerekmektedir. Risklerin belirlenmesi, işletmenin risk profilinin oluşturulmasında ilk adımdır (The Orange Book, 2004: 15). Risklerin belirlenmesi, işletmenin hedeflerine ulaşabilmesinde engel teşkil edebilecek olan risklerin işletme tarafından çeşitli yöntemler kullanılarak belirlenmesi ve gözden geçirilerek güncellenmesini kapsayan bir süreçtir. Risklerin belirlenmesi sürecinde dikkate alınması gereken bazı koşullar söz konusudur. Bunlar (Acar, 2013);

- Belirlenen riskler işletmenin hedefleri ile ilişkili olmalıdır.
- Riskler, işletme tarafından belirlenen yöntemler kullanılarak tespit edilmelidir.

Riskler, işletme hedefleriyle bağlantılı olmalıdır. Tespit edilen bir risk, birden fazla işletme hedefi ile ilgili olabilir, riskin potansiyel etkisi farklı hedeflerle bağlantılı olarak değişim gösterebilir. Önemli olan ise hedeflerle bağlantılı olan risklerin belirlenmesine odaklanarak hedefleri etkilemeyecek risklerin belirlenmesinden kaçınmaktır (The Orange Book, 2004: 15). Ayrıca hedeflere ilişkin olarak tespit edilen riskler iç ve dış riskler olarak sınıflandırılarak hem iç hem de dış riskler de kendi içinde alt sınıflara ayrılmalıdır (Acar, 2013). Özellikle iç riskler işletmeler için oldukça önemlidir. İşletme kültürü, finansal ve operasyonel modüller iç riskleri meydana getirir. Dış çevrede hangi faktörler söz konusu olursa olsun risklerin gerçekleşmesini sağlayan ve etkilerini arttıran yapı işletmelerin içerisidir (Topçu, 2010: 27). İşletmenin dışarıdan sağladığı hizmet alımlarında aksaklık yaşaması, doğal afetlerin oluşma ihtimali, işletmenin web sitelerine yönelik yapılabilecek saldırılar gibi tamamen işletmenin elinde olmayan nedenlerden dolayı karşılaşılabilecek olan riskler ise dış risklerdir (Usul ve Mizrahi, 2016: 14).

Riskler, işletmelerde bir takım risk belirleme teknikleri kullanılarak belirlenmektedir. Teknikler çok çeşitli olmakla birlikte aynı zamanda işletmeden işletmeye de farklılık gösterebilmektedir. Riskler belirlendikten sonra bu risklerden kimin sorumlu olduğu da belirlenmeli ve hazırlanacak risk kaydında bu bilgi de yer almalıdır. Risk yönetimi yapısı gereği dinamik bir süreçtir. Dolayısıyla süreç içerisinde yeni ortaya çıkan risklerin de tespiti yapılmalı ve mevcut risklerde meydana gelen değişiklikler de sürekli olarak takip edilmelidir (Acar, 2013).

3.7. Risklerin Analiz Edilmesi ve Ölçülmesi

Risklerin belirlenmesinin ardından, belirlenmiş olan risklerin analiz edilerek ölçülmesi ve daha sonra elde edilen sonuçlara göre de önceliklendirilmesi aşamaları gerçekleştirilir. İşletme için analiz edilmeden ve ölçülmeden risklerin önem sırasına göre sağlıklı olarak önceliklendirilmesi mümkün değildir ve ancak bu şekilde belirlenen, ölçülen ve önceliklendirilen risklerin işletme içinde etkin bir şekilde yönetilmeleri söz konusudur.

3.7.1. Risk Matrisi

Risk matrisleri, risk yönetiminde basit ancak etkili yaklaşımlar olarak kabul edilmektedirler ve işletmelerde risklerin sistematik olarak gözden geçirilmesi için açık bir çerçeve sağlamaktadırlar (Cox, 2008: 498). Risk matrisi, risklerin değerlendirilmesi esnasında hazırlanır. Risk matrisinin hazırlanmasındaki amaç risklerin olasılıklarının ve etkilerinin doğru ve başarılı bir şekilde tanımlanmasını sağlamaktır.

Risk matrisi ne kadar başarılı hazırlanırsa, risklerin analiz ve ölçümleri de o derece sağlıklı olacaktır (Usul ve Mizrahi, 2016: 37). Öncelikli riskleri belirlemek ve kaynak tahsislerine rehberlik etmek için risk matrislerinin kullanılması ulusal ve uluslararası standartlarda tavsiye edilmiştir. Risk matrisi, kurumsal risk yönetimi ve kurumsal yönetim dâhil olmak üzere risk yönetim danışmanlığı ve uygulamalarının birçok alanına yayılmış durumdadır (Cox, 2008: 498).

Risk matrisi üçlü oluşturulabileceği gibi beşli hatta ikili şekillerde de oluşturulabilmektedir. Mümkün olan en basit risk matrisi 2×2 şeklinde hazırlanan tablodur. Eksenlerin her ikisinin de ikiye bölünmesinden kaynaklanan, satır ve sütunlar "olasılık" ve "sonuç" olarak anılır (Cox, 2008). Ancak uygulamalarda genellikle beşli matrisler tercih edilmektedir (Usul ve Mizrahi, 2016: 36). Şekil 1'de üçlü hazırlanmış bir risk matrisi örnek olarak verilmiştir.

	ETKİ DERECESİ		
İHTİMAL	**1 Düşük**	**2 Orta**	**3 Yüksek**
3 Yüksek	Düşük Etki- Yüksek İhtimal KONTROL FAALİYETLERİ	Orta Etki- Yüksek İhtimal KONTROL FAALİYETLERİ	Yüksek Etki- Yüksek İhtimal KONTROL FAALİYETLERİ
2 Orta	Düşük Etki- Orta İhtimal TOLERE EDİLEBİLİR RİSK	Orta Etki- Orta İhtimal KONTROL FAALİYETLERİ	Yüksek Etki- Orta İhtimal KONTROL FAALİYETLERİ
1 Düşük	Düşük Etki- Düşük İhtimal TOLERE EDİLEBİLİR RİSK	Orta Etki- Düşük İhtimal TOLERE EDİLEBİLİR RİSK	Yüksek Etki- Düşük İhtimal ACİL DURUM EYLEM PLANI

Şekil 1: Risk Önem Düzeyini Gösteren Risk Matrisi (3 x 3)

Kaynak: Derici, 2015: 39-40

3x3 olarak hazırlanan yukarıdaki risk matrisi incelendiğinde yatay sütunların riskin etki derecesinden dikey sütunların ise riskin ihtimal derecesinden bahsettiği anlaşılmaktadır. İhtimaller yüksek, düşük ve orta olarak sıralanmıştır. Risklerin gerçekleşme ihtimallerinin ne anlam ifade ettiği ve her ihtimalin göstergesi aşağıdaki tabloda detaylı olarak açıklanmaktadır.

Tablo 2: Risklerin Gerçekleşme İhtimallerine Göre Değerlendirilmesi

Risklerin Gerçekleşme İhtimallerinin Değerlendirilmesi	
YÜKSEK İHTİMAL	**GÖSTERGELERİ**
Bir yıllık zaman süresi içerisinde gerçekleşme olasılığının bulunması durumudur.	• Gelecek on yıl içinde birçok defa gerçekleşme potansiyeli • Son iki yıl içinde gerçekleşmiş olması • Dış etkenler nedeniyle kontrolün güç olması
ORTA İHTİMAL	**GÖSTERGELERİ**
On yıllık zaman süresi içerisinde gerçekleşme olasılığı bulunması durumudur.	• Gelecek on yıl içinde birden fazla gerçekleşme potansiyeli • Dış etkenler nedeniyle kontrolün güç olması • Faaliyetle ilgili geçmiş deneyimler
DÜŞÜK İHTİMAL	**GÖSTERGELERİ**
On yıllık zaman süresi içerisinde gerçekleşme olasılığının bulunmaması durumudur.	• Şu ana kadar hiç gerçekleşmemiş olması • Gerçekleşmesi halinde büyük bir şaşkınlık durumu yaratacak olması

Kaynak: Derici, 2015: 39-40

Risk matrisinde yatay sütunlar etki derecelerini göstermektedir. Yatay sütunlar incelendiğinde tıpkı ihtimal sütunlarında olduğu gibi etki düzelerinin de yüksek, orta ve düşük olarak sıralandığı görülmektedir. Etki düzeylerinin nitelendirilmesinde kullanılan göstergeler aşağıdaki tabloda verilmiştir.

Tablo 3: Risklerin Etki Düzeylerine Göre Değerlendirilmesi

Risklerin Etki Düzeylerinin Değerlendirilmesi	
ETKİ DÜZEYİ	**GÖSTERGELERİ**
Yüksek Etki	• Kamuoyunun bu riske karşı güçlü bir şekilde duyarlı olması • İşletmenin temel hedefleri üzerinde hayati etkilerinin söz konusu olması • Mali sonuçlarının çok büyük boyutlarda olması
Orta Etki	• Kamuoyunun bu riske karşı önemli ölçüde duyarlı olması • İşletmenin temel hedefleri üzerinde önemli etkilerinin söz konusu olması • Mali sonuçların endişe verici olması
Düşük Etki	• Kamuoyunun bu riske karşı duyarlılığını düşük olması • İşletmenin temel hedefleri üzerinde düşük düzeyde etkili olması • Mali sonuçlarının tolere edilebilir seviyede olması

Kaynak: Derici, 2015: 39-40

3.8. Risklerin Önceliklendirilmesi

Kurumsal risk yönetiminde işletmenin hedefleri üzerinde güçlü etkiye sahip olabilecek kritik risklerin belirlenmesini ve işletmenin sahip olduğu sınırlı kaynakların bu alanlara yoğunlaştırılmasını sağlamak önemlidir. Bu nedenle risklerin kendi içerisinde bir sıralamaya tabi turulması ve önceliklendirilmesi gereklidir. Risklerin önceliklendirilmesinde olasılık etki ve sonuçları gösteren risk matrisi (haritası) kullanılabilir (Ekici, 2015:104).

Risklerin önceliklendirilmesinin amacı nicel ve nitel tekniklerden yararlanılan değerlendirme süreci sonunda işletmedeki hangi risklere daha önce müdahale edilmesine karar verilmesine yardımcı olmaktır. Önceliklendirme, risklerin önem derecelerinin, önceden saptanmış risk ölçütlerinin ve işletmenin risk alma istekliliği ile karşılaştırılmasını ve bu sayede öncelikli olarak dikkate alınması gereken risklerin saptanması sürecini kapsamaktadır (TÜSİAD, 2008: 57).

Riskleri önceliklendirmek bir anlamda risklerin sıralanması demektir (Derici, Tüysüz ve Sarı, 2007: 157). Öncelikli olarak müdahale edilmesi gereken riskler belirlendikten sonra alternatifler dikkate alınarak risk yönetim stratejileri belirlenmektedir (Pehlivanlı, 2010: 84).

3.9. Risk Yönetim Stratejilerinin Seçilmesi

Risk yönetim sürecinin bu aşamasında işletme için geçerli olan her bir riskle mücadele etmede hangi stratejinin kullanılacağına kesin olarak karar vermek oldukça güçtür. Bu kararın verilmesi şüphesiz her işletmeye göre farklılık göstermektedir. Örneğin esnek olmayan ve detaycı bir yönetim politikası benimseyen bir işletme için risk yönetim stratejisine karar verme aşaması sınırlı bir hareket imkânı sunacaktır. Hangi riskte hangi stratejinin riskin yapısına daha uygun olduğu kararını verebilmek için risk yöneticisi potansiyel kaybın ölçüsünü, olasılıkları ve kayıp söz konusu olur ise, tazmin kaynaklarını göz önünde bulundurarak hesaplamak durumundadır. Seçim aşamasında her yaklaşımın kâr ve maliyeti dikkate alınarak değerlendirilir (Emhan, 2009: 215).

Risk yönetim stratejilerini aşağıdaki gibi bir sınıflandırmaya tabi tutmak mümkündür.

- **Kaçınma (Avoidance):** Riske neden olan iş birimini satmak, endişe veren bir coğrafi bölgeden çıkmak ya da bir ürün grubunu bırakmak gibi faaliyetler yoluyla işletmenin riskten uzak durma durumudur. Buradaki zorluk ise genellikle riskin ilgili maliyetleriyle birlikte gerçekleşmesine dek işletmelerin ürün hattının bırakmaması ya da iş biriminden uzaklaşamamasıdır. İşletme çok düşük risk iştahına sahip olmadıkça, diğer bütün koşullar hali hazırda yolundayken sadece gelecekteki potansiyel risk temeline dayanarak bir faaliyet alanından çıkması ya da ürün grubundan uzaklaşması oldukça zordur. Öte yandan eğer herhangi bir yatırım gelecekte daha büyük bir riski önlemeye yarayacak bir alana girmek için yapılıyorsa bu defa kaçınma stratejisi potansiyel olarak daha maliyetli bir strateji olacaktır (Moeller, 2011: 74).

- **Azaltma (Reduction) :** Bu tutumda risk olasılığını, etkisini veya her ikisini de azaltmak için harekete geçilmesi kastedilmektedir. Gerekli ve uygun kontroller ile risklerin olumsuz etkilerinin gerçekleşme olasılıklarının azaltılmasına ya da risklerin olumsuz etkilerinin derecesinin azaltılmasına yönelik gerçekleştirilen faaliyetlerdir (TÜSİAD, 2008: 60). Örneğin bir finans işletmesi, sistemleri-

nin üç saatten fazla çalışmama riskini belirleyerek değerlendirdiğinde böyle bir olayın etkisini kabul edemeyeceğine karar verebilir. Bu durumda işletme bu olasılığı azaltmak için gelişmiş yedekleme sistemleri ile teknolojiye yatırım yapma yoluna gidebilir (COSO, 2004: 55).

- **Paylaşma (Transfer Etme) (Sharing) :** Bu tutum, riski bir varlıktan diğerine taşımayı içermektedir (Marchetti, 2012: 29). Paylaşma tutumunda riskin tümünün ya da bir kısmının başka bir tarafça üstlenilmesi durumu söz konusudur (TÜSİAD, 2008: 60). Hemen hemen tüm işletmeler düzenli olarak risklerinden korunmak ya da risklerini paylaşmak için örneğin sigorta yaptırma yolunu tercih ederler. Paylaşma tutumunda sigorta yaptırma yönteminden başka çeşitli farklı teknikler de mevcuttur (Moeller, 2011: 75). Bu paylaşım teknikleri içinde çeşitli anlaşmaların kullanılması, ortaklıklar kurma gibi yapılanmalar da sayılabilmektedir. Çoğunlukla riskin paylaşılması esnasında bir maliyet ortaya çıkacaktır (sigorta için prim ödenmesi gibi). Bu sebeple riskin paylaşılması kararlarında fayda-maliyet analizi yönetim tarafından dikkatlice gerçekleştirilmelidir. Riskin paylaşılma tutumu ile birlikte başka bir risk de alınmış olmaktadır. Bu risk, riski üstlenmiş olan tarafın riski uygun ve etkin bir şekilde yönetememesinden kaynaklanacak risktir (TÜSİAD, 2008: 60-61).
- **Kabul Etme (Göze Alma) (Acceptance) :** İşletme yönetimi, zaman zaman işletmede sürdürülen faaliyetlerin doğası gereği bir takım kaçınılmaz riskleri kabul etmek durumundadır. Ayrıca bazı durumlarda fayda-maliyet analizi uygulandığında riski azaltmak için gereken maliyet, onu üstlenmek için gereken maliyetten daha yüksek olduğu tespit edilirse bazı riskler kabul edilebilir (Marchetti, 2012: 29). İşletmede var olan çeşitli riskler için birçok tutum tercih edilebilirse de kabul etme tutumu çoğu zaman bazı riskler için en uygun stratejidir (Moeller, 2011: 75). Şüphesiz yönetimin kabul ettiği riskler (risk toleransı dâhilinde) risk yönetimi sürecinde de izlenmelidir (Marchetti, 2012: 29).

Yukarıda bahsi geçen dört çeşit stratejiye ilave olarak alternatif bir çeşit olmamakla birlikte azaltma, kabullenme ya da paylaşma seçenekleri ile bir arada kullanılabilecek "Fırsatları Değerlendirme" seçeneği de bazı kaynaklarda yer almaktadır. Buna göre fırsatları değerlendirme stratejisinde riskin tamamen ortadan kaldırılması mümkün olmasa da olumsuz etkilerini azaltmak için bazı fırsatlar değerlendirilebilir. Öte yandan işletme faaliyetleri ile ilgili olan alanlarda kimi zaman işletmenin başarısını arttıracak fırsatlar ortaya çıkabilir**.** Ortaya çıkan bu tarz fırsatların değerlendirilebilmesi için işletmenin önceden bir stratejiye sahip olması ve belirlediği stratejiye uygun faaliyetlerde bulunması, fırsatlardan yararlanabilme olanağını arttırmaktadır (Derici, 2015: 22).

3.10. Bilgi ve İletişim

Risk yönetimi faaliyetlerinin sıklıkla soyut şekilde yürütülüyor olması nedeniyle işletme içerisinde risk iletişimi için gereken iç mekanizmalar sağlıklı olarak işletilebilmelidir (Bolgün, 2010: 6). İşletme içerisinde etkili bir iletişim sağlanabilmesine yönelik olarak çalışanların risk yönetimine dair görüşleri, öneri ve eleştirilerini karşılıklı olarak paylaşabilecekleri ortamlar düzenlenebilir. Çalışanların faaliyetleri sırasında karşılaştıkları problemleri ya da paylaşmak istedikleri bilgileri ast ve üstleri ile nasıl bir iletişim kanalı ve yöntemi kullanarak paylaşacakları açık bir şekilde işletmede ifade edilmelidir. Tüm çalışanlar, bu iletişim kanallarını kullanabilecekleri konusunda bilgilendirilmelidir (Derici, 2015: 57).

3.11. Sürekli İzleme

Risk yönetim faaliyetlerinin, kendisinden beklenen amaca yönelik ve güncel içeriğe sahip olması için yürütülecek sürekli izleme uygulamaları önemlidir. İşletmeler faaliyetlerini sürdürürken değişen zamanla birlikte işletme için söz konusu olan risklerin etki derecelerini ve olasılıklarını etkileyen faktörler de değişim göstermektedir. Bu duruma bağlı olarak yürütülen risk yönetim faaliyetlerinin de etkileri ve maliyetleri değişmektedir. Bütün bu nedenler kurumsal risk yönetim sürecinin sistematik ve sürekli olarak izlenmesini gerektirmektedir (Günbey, 2008: 102). İzleme fonksiyonu işletmelerde, sürekli izleme ve münferit izleme olarak iki şekilde gerçekleşebilir. Risk yönetiminin hızlı değişime uygun yapısı nedeniyle riskler sürekli izlenebilirken, işletmenin tercih etmesi halinde belirli bir riskin tek olarak ele alınması olarak ifade edilen münferit izleme işletmelerde uygulanabilir (Derici, 2015: 58).

Kurumsal risk yönetim sürecinin etkin ve sürekli olarak izlenebilmesi ve sürecin geliştirilmesine yönelik önerilerinin oluşturulabilmesi için her aşamanın uygun şekilde belgelenerek kayıt altına alınması gerekmektedir. Yöntem ve varsayımlar, bilgi kaynakları, analizler, analiz sonuçları ve alınan kararların nedenleri, belgelenmesi gereken temel konular arasındadır. Sürecin kayıt altına alınarak belgelenmesinde aşağıda sıralanan temel ilkeler göz önünde bulundurmalıdır (TÜSİAD, 2008: 63):

- Ticari ve yasal kayıt gereksinimleri,
- Kayıtların oluşturulması ve elde tutulması maliyetleri,
- Bilginin tekrar kullanılması

Yöneticiler, işletmelerinin kendilerine has yapısal özelliklerini dikkate aldıklarında, kurumsal risk yönetim yapısı oluşturmak için geliştirilecek süreç ve metodoloji ile ilgili seçim yapmak durumunda kalırlar. Kimi yöneticiler kurumsal risk yönetimi aşamalarında belirli iş birimleri için karmaşık ve detaylı teknikler izlerken kimileri kurumsal risk yönetimi uygulama yapılarında daha genel ve basit bir yaklaşım benimseyebilirler (Yılmaz, 2007: 103). Bu noktada önemli olan seçilecek ve uygulanacak kurumsal risk yönetim yapısının işletmenin özelliklerine uygun ve ihtiyaçlarına cevap verebilecek şekilde belirlenebilmesidir.

4. SONUÇ VE DEĞERLENDİRME

Kurumsal risk yönetim sistemi işletmeye şüphesiz yüzde yüz bir güvence sağlayamamaktadır. Çünkü kurumsal risk yönetim sistemi işletmelerde ne kadar iyi kurulmuş olursa olsun karar verme sürecinde risk değerleme ve tutumlarına ilişkin alınan kararlarda insan doğasından kaynaklanabilecek bazı hatalar söz konusu olabilmektedir. Risk geleceğe ilişkin bir olgudur ve gelecek de belirsizlik barındırır. Dolayısıyla risk yönetiminde önceden kesin ve net bir tahmin yapılamamaktadır. Ancak işletmelerde kurumsal risk yönetim sürecinin etkin olarak uygulanması, faaliyetlerle ilgili daha bilinçli kararlar alınması ve işletmede risk yönetimi ile ilgili olarak daha sağlıklı iletişim kurulması gibi konular da dâhil olmak üzere işletmenin gelişimine katkıda bulunmaktadır.

İşletmelerde kurumsal risk yönetimi sürecinde oluşturulacak uygulama adımları, işletmenin dış çevresi, faaliyette bulunduğu endüstri kolu, faaliyetleri, organizasyonel yapısı, büyüklüğü, teknik alt yapısı, sahip olduğu yönetim ve insan kaynakları politikaları gibi faktörler ile yakından ilgilidir. Bu nedenle her

işletme kendi yapısına en uygun modeli oluşturacak ve uygulanan modeller işletmeden işletmeye farklılık gösterir nitelikte olacaktır. Bu çalışmada işletmelerde kurumsal risk yönetim sisteminin kurulması ve etkin şekilde sürdürülebilmesi için uygulanması gereken adımları ve adımların her birinde yürütülmesi gereken faaliyetleri içeren kurumsal risk yönetim süreci ele alınmıştır. Kurumsal risk yönetimi uygulama sürecine yer veren çeşitli çalışmalar incelenmiştir. Yapılan inceleme sonucunda sürecin ana hatlarının benzer olmasıyla birlikte incelenen her çalışmada adımların birebir aynı olmadığı görülmüştür. Bu durumun kurumsal risk yönetim sistemine ait genel kesin bir yapının var olmamasından ve her araştırmacının kurumsal risk yönetim sürecinin yapısına kendi yorumu ile yaklaşmasından kaynaklı olduğu söylenebilir. Çalışmalardan elde edilen bilgiler ışığında sürece yönelik izlenebilecek on bir adımı içeren bir model oluşturulmuştur. Tablo 1'de yer verildiği üzere mevcut literatürde bazı çalışmalarda kurumsal risk yönetimi adımları içerisinde dış ve iç unsurların belirlenmesi adımlarının yer almadığı görülmektedir. Bu çalışmada ise kurumsal risk yönetimi sürecinin başlangıç adımını dış unsurların belirlenmesi adımı, ikinci adımını ise, iç unsurların belirlenmesi adımı oluşturmaktadır. Çünkü dış ve iç unsurların belirlenmesi adımlarının işletmede kurumsal risk yönetimi sürecinin başarısı için önemli rol oynadığı düşünülmektedir. Özellikle iç unsurların belirlenmesi adımında yer alan vizyon ve misyon hakkında bilgi sahibi olmak ve işletmede hali hazırda işleyen risk yönetim sisteminin durum analizini yapmak yoluyla güçlü ve zayıf yönlerini belirlemek kurumsal risk yönetimi sürecinin sağlıklı şekilde kurularak sürdürülmesi için önemlidir. Üçüncü adım olarak hedeflerin belirlenmesi adımına yer verilmiştir. İşletme hedeflerinin belirlenmesinin ardından tüm çalışanların rol ve sorumluluklarının belirlendiği bir kurumsal risk yönetimi çerçevesinin işletmede oluşturulması gereklidir. Risklerin belirlenmesi adımından önce işletme, kabul etmeye hazır olduğu risk miktarını gösteren risk iştahını da belirlemelidir. Risk iştahının belirlenmesinin ardından kurumsal risk yönetim sürecinin esas konusunu oluşturan risklerin belirlenmesi adımına geçilmelidir. Belirlenen riskler, işletmede hazırlanacak risk matrisleri yardımıyla analiz edilerek ölçülmelidir. Analizi yapılarak ölçülen riskler belirli bir sıralamaya tutularak önceliklendirilmelidir. Bu anlamda risklerin önceliklendirilmesi sekizinci adımı oluşturmaktadır. Risklerin yönetilebilmesi için çeşitli risk yönetim stratejileri söz konusudur. Dokuzuncu adım, işletmenin karşı karşıya olduğu riskleri için hangi risk yönetim stratejilerinin seçileceğine karar verilmesi gereken adımdır. Kurumsal risk yönetim sürecinde risk yönetim faaliyetlerinin sürdürülmesinde işletmede iletişim kanallarının kullanılması yoluyla bilgi akışı da sağlanmış olmalıdır. Ayrıca son adım olarak açıklanan sürecin sürekli izlenmesi adımı sayesinde de sürecin geliştirilmesi mümkün olabilecektir.

Çalışmada detaylı olarak açıklanan on bir adım kurumsal risk yönetimi uygulama sürecine yönelik tavsiye niteliği taşımaktadır. Bahsi geçen adımların sayısının ve sıralamasının işletmelerin yapılarına göre farklılık gösterebilmesi mümkündür. Ancak burada esas dikkat edilmesi gereken nokta işletmelerin kendi yapılarına uygun olan kurumsal risk yönetimi uygulama sürecini kurgulayabilmesi ve süreçte yer alacak ana prensiplerin ve uygulanması gereken adımların belirlenen hedefler ile uyumlu olacak şekilde yürütülebilmesidir. Öte yandan kurumsal risk yönetimi sürecinin uygulanması aşamasında kim, ne, nasıl, nerede ve ne zaman sorularının yanıtlarını oluşturacak şekilde ayrıntılı bir planın hazırlanması da sürecin amaca uygun yürütülmesi açısından önemlidir.

KAYNAKÇA

Acar, Şafak Birol, Risk Yönetimi ve Kontrol Faaliyetleri, Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü Mali Yönetim ve Kontrol Dairesi, Bolu, 9-10 Mayıs 2013.

Arslan, Işılda, Kurumsal Risk Yönetimi, Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Mart, 2008.

COSO, Enterprise Risk Management- Integrated Framework, Executive Summary Framework, September, 2004.

Cox, Louis Anthony (Tony), "What's Wrong with Risk Matrices?", Risk Analysis, Vol. 28, No.2, 2008, s.497-512.

Derici, Onur, İç Kontrol ve Risk Yönetimi, BEKAD Yayınları, Yayın No:21, Antalya, 2015.

Duran, Erdal, Kamu İdarelerinde Kurumsal Risk Yönetimi Uygulamaları, Mali Hizmetler Uzmanlığı Araştırma Raporu, Ankara, Aralık 2013.

Dickinson, Gerry, "Enterprise Risk Management: Its Origins and Conceptual Foundation", The Geneva Papers on Risk and Insurance Vol. 26, No. 23, July 2001, s. 360-366.

Ekici, Hasan, Kurumsal Risk Yönetimi, Konya, Çizgi Kitabevi, 2015.

Emhan, Abdurrahim, "Risk Yönetim Süreci ve Risk Yönetmekte Kullanılan Teknikler", Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, Cilt: 23, Sayı: 3, 2009, s. 209-220.

Göğüş, Handan Sümer, Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi, Türkmen Yayınları, İstanbul, 2015.

Günbey, Ahmet, Kurumsal Risk Yönetiminde İç Denetimin Rolü ve Bir Uygulama, Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kütahya, 2008.

Güneş, Şule, Kurumsal Risk Yönetimi ve Türkiye'de Farkındalığına İlişkin Bir Uygulama, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2009.

IMA (Institute of Management Accountants), Enterprise Risk Management: Tools and Techniques for Effective Implementation, 2007.

Kılıç, Mustafa, "Stratejik Yönetim Sürecinde Değerler, Vizyon ve Misyon Kavramları Arasındaki İlişki", Sosyoekonomi Dergisi, Temmuz-Aralık 2010-2, s. 81-98.

Kızılboğa, Rüveyda, Kurumsal Risk Yönetimi Odaklı İç Denetim İstanbul Büyükşehir Belediyesi için Bir Model Önerisi, Marmara Belediyeler Birliği, 2013.

Lam, James, Enterprise Risk Management From Incentives to Controls, John Wiley & Sons, New Jersey, 2003.

Marchetti, Anne A., Enterprise Risk Management Best Practices, John Wiley & Sons, New Jersey 2012.

Olson, David L. ve Desheng Wu, Enterprise Risk Management in Finance, Palgrave Macmillan, 2015.

Saka, Tamer, Kurumsal Risk Yönetimi ve 2008 Yılı Risk Öngörüleri, TÜSİAD, 21 Şubat 2008. tusiad.org/tr/tum/item/download/2468_47d48b480878ef141e0ded0518703d78, Erişim Tarihi: 24.01.2018.

Sarpkaya, Duygu, Kurumsal Risk Yönetiminde İç Denetimin Rolü, İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2012.

The Orange Book: Management of Risk-Principles and Concepts, United Kingdom (UK): HM Treasury, October, 2004.

Topçu, Bünyamin, Finans Dışı Şirketlerde Kurumsal Risk Yönetimi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul, 2010.

TÜSİAD Risk Yönetimi Çalışma Grubu, Kurumsal Risk Yönetimi, Yayın No. TÜSİAD-T/2008-02/452, 2008.

Usul, Hayrettin ve Rozi Mizrahi, Risk Odaklı Denetim, Detay Yayıncılık, Ankara, 2016.

Yılmaz, Ayşe Küçük, Havaalanlarında Kurumsal Risk Yönetimi Atatürk Havalimanı Terminalleri İşletmesi için Kurumsal Risk Yönetimi Model Önerisi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi, Eskişehir, 2007.