T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME YÖNETİMİ BİLİM DALI

FİNANS DIŞI ŞİRKETLERDE KURUMSAL RİSK YÖNETİMİ VE ÖRNEK RİSK MATRİSİ UYGULAMASI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Hüseyin AĞGÜL

İstanbul, 2019

T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İŞLETME YÖNETİMİ BİLİM DALI

FİNANS DIŞI ŞİRKETLERDE KURUMSAL RİSK YÖNETİMİ VE ÖRNEK RİSK MATRİSİ UYGULAMASI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Hüseyin AĞGÜL

Öğrenci No:

17550458016

Danışman:

Dr. Öğretim Üyesi Mustafa SUNDU

İstanbul, 2019

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "**FİNANS DIŞI ŞİRKETLERDE KURUMSAL RİSK YÖNETİMİ VE ÖRNEK RİSK MATRİSİ UYGULAMASI**" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmanın içinde kullanıldıkları her yerde bunlara atıf yapıldığını, çalışmada örnek olay olarak incelenen firmadan izin alındığını ve firmanın talebi üzerine yer ve isim bilgilerine metinde yer verilmediğini belirtir ve bunu onurumla doğrularım. 17/04/2019

Hüseyin AĞGÜL

T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ
TEZLİ YÜKSEK LİSANS SINAV TUTANAĞI

17/04/2019

Enstitümüz ***İşletme*** Anabilim Dalı ***İşletme Yönetimi*** Programı yüksek lisans öğrencilerinden **17550458016** numaralı ***Hüseyin AĞGÜL'***ün *"Beykent Üniversitesi Lisansüstü Eğitim – Öğretim Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"Finans Dışı Şirketlerde Kurumsal Risk Yönetimi ve Örnek Risk Matrisi Uygulaması"*** konulu tezini, Yönetim Kurulumuzun 02/04/2019 tarih ve 2019/14 sayılı toplantısında seçilen ve Taksim Yerleşkesinde toplanan biz jüri üyeleri huzurunda, Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 29. maddesinin 3. fıkrası gereğince (67) dakika süre ile aday tarafından savunulmuş ve sonuçta adayın tezi hakkında ~~***oyçokluğu/oybirliği***~~ ile ***Kabul/~~Red veya Düzeltme~~***
kararı verilmiştir.

İşbu tutanak, 4 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
Dr. Öğr. Üyesi Mustafa SUNDU
(Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi Okan YAŞAR
(Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi Sulhi ESKİ
(İstanbul Gelişim Üniversitesi)

Adı ve Soyadı : Hüseyin AĞGÜL
Danışmanı : Dr. Öğretim Üyesi Mustafa SUNDU
Türü ve Tarihi : Yüksek Lisans Tezi, 2019
Alanı : İşletme Yönetimi
Anahtar Kelimeler : Kurumsal Risk Yönetimi, Risk Matrisi, TTK

ÖZ

FİNANS DIŞI ŞİRKETLERDE KURUMSAL RİSK YÖNETİMİ VE ÖRNEK RİSK MATRİSİ UYGULAMASI

Dünya'da gelişen ve entegre olan finansal piyasalar, bunu takip eden türev ürünler ve spekülatif hareketler, borsa ve denetim skandalları, gittikçe tırmanan gelir dağılımı bozukluğunun da etkisiyle şıklaşan yöresel savaşlar ve terör olayları, iklim değişikliğinin getirdiği büyük ölçekli belirsizlikler ve doğal felaketler risk yönetiminin önemini artırmıştır. Buna bağlı olarak önce toplam kalite kontrol adı altında gelişen, sonra kurumsal yönetim ilkelerini kapsayan ve en son kurumsal risk yönetimi olarak adlandırılan yönetim şekli gelişen ülkeler başta olmak üzere gerekli yasal düzenlemeler ile finansal sektör dışında da şirketler için zorunlu hale getirilmeye başlanmıştır. Türkiye'de ise şirketler kesimi çok dinamik olsalar da, sürdürülebilir bir büyüme için gerekli kurumsal risk yönetimini uygulamalarına geçmekte ve entegre risk yönetimi kültürünü oluşturmakta zorlanmaktadırlar.

Bu tezde, kurumsal risk yönetimi ve Türkiye'deki yasal düzenlemeler hakkında bilgi verdikten sonra, son yıllarda hızlı büyüme kaydeden sanayi ve perakende sektöründe faaliyet gösteren bir firmanın risk yönetimi uygulamaları değerlendirilecektir. COSO risk değerlendirme formuna verilen cevaplar ve içsel kurumsal risk yönetimine ait belgeler ışığında, şirketin vizyonu, stratejik ve operasyonel hedefleri, risk eğilimi, risk toleransına göre özet bir risk matrisi yer verilmiştir. Şirket ile ilgili yapılan niteliksel araştırma sonuçları, şirketin iç denetim departmanı aracılığıyla risk yönetimi yaptığını ve henüz şirket içi risk kültürünün oluşmadığını göstermiştir. Şirketin yüksek stratejik hedeflerine ulaşması için şirketin daha kurumsallaşması ve risk yönetimine daha fazla önem vermesi gerektiği düşünülmektedir.

Name and Surname : Hüseyin AĞGÜL
Supervisor : Dr. Lecturer Mustafa SUNDU
Degree and Date : Master Thesis, 2019
Major : Business Administration
Key Words : Enterprise Risk Management, Risk Matrix, TTK

ABSTRACT

ENTERPRISE RISK MANAGEMNET IN NON-FINANCIAL FIRMS AND AN APPLICATION OF RISK MATRIX

Globally advanced and integrated financial markets complicated by derivative products and speculative movements, audit scandals, frequent regional distresses and terrorist attacks triggered by uprising disparity in income distribution, large-scale uncertainties and natural disasters caused by climate change amplified the importance of risk management. In this respect, primary implementation of risk adjusted management appeared under Total Quality Control, then evaluated through corporate governance principles to integrated corporate risk management. Under the leadership of developed countries, spreading over legal developments and regulations in this area are pushing the reel sector companies to apply integrated risk management. In Turkey, even though the corporate sector is very dynamic, the firms are struggling to apply corporate risk management, as well as to create integrated risk management.

In this thesis, after giving information about enterprise risk management and legal regulations in Turkey, we analyzed corporate risk management applications of a firm acting in industrial and retail sectors which has been growing significantly in recent decade. In the light of the questionnaire and internal corporate risk management documents, the company's corporate risk management practices including the company's vision, strategic and operational objectives, risk appetite and risk tolerance evaluated in the form of risk matrix. We found out that, the firm apply risk management throughout internal audit department. Furthermore the firm has a basic risk management implementation lacking an integrated risk management culture. In order to achieve its ambitious strategic aims, the firm should adopt more institutional management skills with an apparent emphasis on integrated risk management.

İÇİNDEKİLER

Sayfa No.

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

ABD : Amerika Birleşik Devletleri
AIRMIC : Sigorta ve Risk Yöneticileri Derneği
ALARM : Kamu Sektörü Risk Yönetimi Ulusal Forumu
AS/NZS 436 : Avustralya/Yeni Zelanda Standardı -
BDDK : Bankacılık Düzenleme ve Denetleme Kurumu
BIS : Bank for International Settlements
COSO : Committee of Sponsoring Organizations of the Treadway Commission
ÇSGB : Çalışma ve Sosyal Güvenlik Bakanlığı
ERM : Enterprise Risk Management
ERP : Kurumsal Raporlama Platformu
ESG : Environmental, Social and Governance
EWF : European Federation for Welding, Joining and Cutting
FERMA : Avrupa Risk Yönetimi Dernekleri Federasyonu
FMEA : Failure Mode and Effect Analysis
HAZOP **:** Hazard and Operability Analysis
ISO : Uluslararası Standartlar Kurumu
IRM : Risk Yönetim Enstitüsü
KRI : Kritik Risk İndikatörleri
KRY : Kurumsal Risk Yönetimi
OECD : Organization for Economic Cooperation and Development
PESTLE : Politics, Economics, Sociologic, Technologic, Ecologic, Legal Analysis
PWC : Price Waterhouse Coopers
RMD : Riske Maruz Değer
SEC : Securities and Exchange Commission
SPK : Serbest Piyasa Kurulu
SYR : Sermaye Yeterliliği Raporu
SWOT : Strength, Weakness, Opportunity, Threat Analysis
TTK : Türk Ticaret Kanunu
TÜSİAD : Türk Sanayici ve İşadamları Derneği

GİRİŞ

Teknolojik gelişmelerle birlikte gittikçe iç içe geçen ve karmaşıklaşan ekonomik yapı, küreselleşmenin ötesinde entegrasyon getirmekte, artan rekabet, yasal düzenlemeler ve gittikçe sıklaşan ve derinleşen konjonktür döngüleri (business cycles) şirketlerin önemli ve karmaşık riskler ile karşı karşıya bırakmaktadır. Değişen ekonomik ve teknolojik koşulların yarattığı riski bulunan kurumların mevcut durumunu, devamlılığını ve gelişimini olumsuz etkileyebileceği gibi kurumlara önemli fırsatlar da sunmaktadır. Risklerin yarattığı fırsatları da değerlendirebilmek için risklerden kaçınmak değil riskleri yönetmek önemlidir. Risklerin başarıyla yönetilmesi işletmelerin karlılığını artırarak başarısını ve devamlılığını artırmaktadır. Risklerin yönetilmesi ise maruz kalınan risklerin tanımlanması ve boyutlarının analiz edilmesi, en etkin aksiyonların alınması, olabilecek kayıpları minimum düzeye indirilmesi ve fırsatların en iyi şekilde değerlendirebilmesini sağlayacak politikaların gelişebilmesine bağlıdır.

Dünya'da gelişen ve entegre olan finansal piyasalar, bunu takip eden türev ürünler ve spekülatif hareketler, borsa ve denetim skandalları, gittikçe tırmanan gelir dağılımı bozukluğunun da etkisiyle şıklaşan yöresel savaşlar ve terör olayları, iklim değişikliğinin getirdiği büyük ölçekli belirsizlikler ve büyük çaplı doğal felaketler gelişen ülkelerdeki yasa düzenleyicileri ve şirket yönetimini etkilemiştir. 1970'li-1980'li yıllarda Japon odaklı ve daha çok imalat sektörüne yönelik toplam kalite yönetimi (total quality management) daha sonra süreç yönetimini de kapsayacak şekilde hizmet sektörüne de uygulanmış, daha sonra borsa skandalları ile kurumsal yönetim ve denetim (corporate governance and auditing) olarak geliştirilmiş ve en son risklerin daha da karmaşıklaşması ve küreselleşmenin sonucu krizlerin büyük bir hızla yayılması sonucu bütün bu kavramların birleştiği kurumsal risk yönetimine (Entreprise risk management) geçilmiştir.

Türkiye'de ise tasarruf yetersizliği ve teknolojik gereksinimden dolayı dışa bağımlı bir ekonomi ve buna bağlı olarak dış gelişmelerden çok hızlı etkilenen bir şirketler kesimi vardır. Ekonomik yüksek dışa bağımlılığı, şirketler kesimi için dalgakıran sız yapılmış ve açık denizin bütün fırtınalara maruz kalan bir marinadaki büyüklü küçüklü tekneler çağrışımı yapmaktadır. Dolayısıyla bir çok işletme, döviz, faiz

ve uluslararası emtia fiyatlarındaki dalgalanmalar, yatırımların kısa vadeli kredilerle finanse edilmesi, yetersiz öz kaynak, döviz üzerinde spekülasyonların meydana getirilmesi ve dövizde açık pozisyon, terör olayları ve politik dalgalanmalar ve benzer nedenlerle direk ve yüksek miktarda risklerle karşı karşıya kalabilmektedir. Sanayileşmesi gelişmiş ve istikrarlı piyasalarda bile dalgalanmalara neden olan terör ve finansal krizler (subprime crisis) direk ülkemizi etkilemekte, içte yaşanan ekstra belirsizlikler birleşip Türk işletmelerini zor duruma sokmakta ve kolayca iflasa sürüklemektedir.

Türk şirketleri içinde bulundukları yapısal bozukluklarla birlikte, ülkenin 1990'larda hızlı serbest piyasa ekonomisine geçmesinin getirdiği kırılgan ekonomik yapı ve birbiri arkası gelen krizlerin getirdiği dalgalanmalara karşın kısa dönemli planlar ile yaşamaya alıştırmıştır. Her ne kadar kısa dönemli karar mekanizmasına alışan şirketler çok dinamik olsalar da, sürdürülebilirlik için geçerli ve uzun dönemli karar alma sürecini gerektiren kurumsal risk yönetimini uygulamalarına geçmekte zorlanmaktadırlar. Bilhassa reel sektör şirketleri, risklerini belirlemede ve ölçmede, gerek teknik altyapı gerekse uzman personel açısından oldukça yetersiz kalmaktadırlar. Dolayısıyla şirketler kesimi piyasalarda meydana gelen en küçük bir değişimden ya da belirsizlikten hızlı ve büyük ölçüde etkilenmekte ve bu etkilerden korunamamaktadırlar.

Özellikle halka açık şirketlerde uygulanması zorunlu olan kurumsal yönetimin bir gereği olarak görülen kurumsal risk yönetimi ile ilgili olarak özellikle gelişmiş ülkelerde düzenlemeler yapılmış, risk yönetimine dair birçok mevzuat ve standart oluşturulmuş ve uygulamaya konulmuştur. Türkiye'de risk yönetimi ile ilgili ilk düzenlemeler 2001 yılında yaşanan ikiz krizle (bankacılık ve reel sektör krizi) birlikte olmuştur. Bankacılık sektöründeki bariz açık pozisyon, sermaye yetersizliği ve karşılıksız alacaklar (Non-performing loan) tahammül edilemeyecek noktaya geldiği için yaşanan likidite, kredi daralması ve döviz kurlarındaki aşırı yükselme (devaluation) reel sektöründe krize girmesine neden olmuştur. Krizden çıkmak için zorunlu olarak riskin önceden belirlenmesi ve yönetimiyle ilgili ilk düzenleme yeni oluşturulan Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 8 Şubat 2001 tarihli "Bankaların İç Denetim ve Risk Yönetim Sistemleri Hakkında Yönetmelik" ve 10 Şubat

2001 tarihli "Bankaların Sermaye Yeterliliğinin Ölçülmesi ve Değerlendirilmesine İlişkin Yönetmelik" ile uygulanmıştır.

Finansal sektörde sistemik riskin tesirlerini azaltmak amacıyla yapılan yönetmelikler ve uygulamada zorlama ile bankalarda risk yönetim sistemleri alt yapısı belirlenmiş ve sektörün uygun bir sisteme girmesi için önemli adımlar atılmıştır. Bankacılık sektöründe oluşturulan risk yönetimi kültürünü şirketler kesiminde de yaygınlaştırmak için 30 Aralık 2011 tarihli Resmi Gazete 'de yer alan "Kurumsal Yönetim İlkelerinin Belirlenmesine ve Uygulanmasına İlişkin" Tebliğ yayınlanmıştır. Bu tebliğe göre işletmelerin yönetim kurulu bünyesinde kurması gerekli komiteler içine denetimden sorumlu komite, kurumsal yönetim komitesinin, aday gösterme komitesi, riskin önceden tespiti komitesi ve ücret komitesi eklenmiştir. Fakat Tebliğ ile halka açık anonim şirketlerde riskin erken saptanmasına ve yönetilmesine ilişkin gerekli komitenin yönetim kurulunca kurulması hükme bağlanmıştır. Herhangi bir yaptırım getirilmemiştir. Risk yönetimine ilişkin son düzenleme ise 2011 yılında yasalaşan 6102 sayılı Türk Ticaret Kanunu ile yapılmıştır. Bu konu alt başlık olarak daha detaylı incelenecektir. Kanuni düzenlemelere rağmen uygulamada sadece düzenlemeye uyum için komiteler kurma çabaları gözükmektedir ve şirketler kısmında etkin bir kurumsal risk yönetimi kültürü oluşmuş gözükmemektedir.

İçinde bulunduğumuz dönemde yani 2018-2019 yıllarında zor duruma düşen şirketlerin sayısındaki artış göz önüne alınarak, bu tez zor ekonomik koşullar çerçevesinde artan kurumsal risk yönetiminin önemine dikkat çekmek amacıyla hazırlanmıştır. Bu tez zorlu gerek teorik bilgilere gerekse uygulamaya yönelik bilgiler verilecektir. Birinci bölümde risk ve kurumsal risk yönetimi hakkında teorik bilgi verilecek, daha sonra kurumsal risk yönetimin önemli bileşenlerinden olan kurumsal yönetim ve iç denetim hakkında kısa bir teorik bilgi verilecektir. İkinci bölümde Türkiye'deki düzenlemelere ve uygulamalara yer verecektir. Üçüncü bölümde kurumsal risk yönetimi standartları, kurumsal risk yönetiminin aşamaları ve uygulama metodolojileri hakkında teorik bilgi verilecektir. Özellikle uygulama bölümünde kullanacağı için COSO - Treadway Komisyonu Sponsor Kuruluşlar Komitesi Kurumsal Risk Yönetimi Çerçevesi konusunda detaylı bilgi verip, bu çerçevenin bir parçası olan Risk Yönetimi Değerlendirme formu tanıtılacaktır. En son bölümde saha araştırmasına

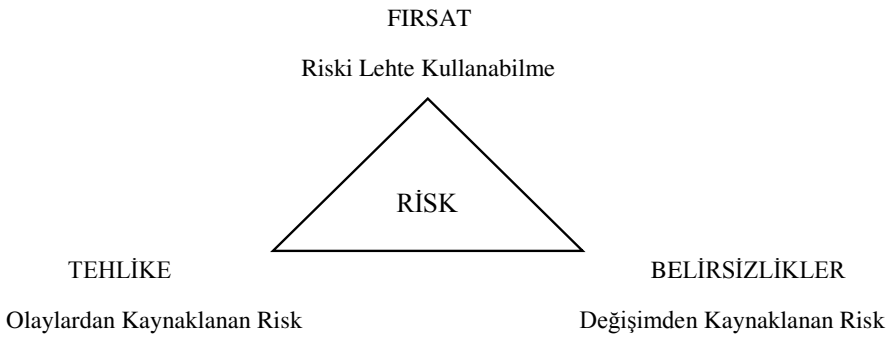
yer verilecek ve elde edilen veriler üzerinde risk matrisi çıkarılacaktır. Son yıllarda hızlı büyüme kaydeden bir firma tarafından cevaplanan risk değerlendirme formu ve içsel kurumsal risk yönetimine ait belgeler ışığında, kurumsal risk yönetimi aşamalarına göre, şirketin kurumsal risk yönetimi uygulamaları değerlendirilecektir. Ayrıca şirket içinde doldurulacak risk değerlendirmesi formu sonuçları ışığında şirketin vizyonu, stratejik ve operasyonel hedefleri, risk eğilimi, risk toleransı, risklerin değerlendirilerek alınacak aksiyonları içeren özet bir risk matrisini çıkarılacaktır.

1. RİSK VE KURUMSAL RİSK YÖNETİMİ

Bu bölümde kurumsal risk yönetimi ile ilgili teorik bilgiler verilecektir. Teorik verilere geçmeden önce risk, risk yönetimi, kurumsal yönetim ve iç denetim ile ilgili kavramlar açıklanacaktır.

1.1. Genel Olarak Riskin Tanımı

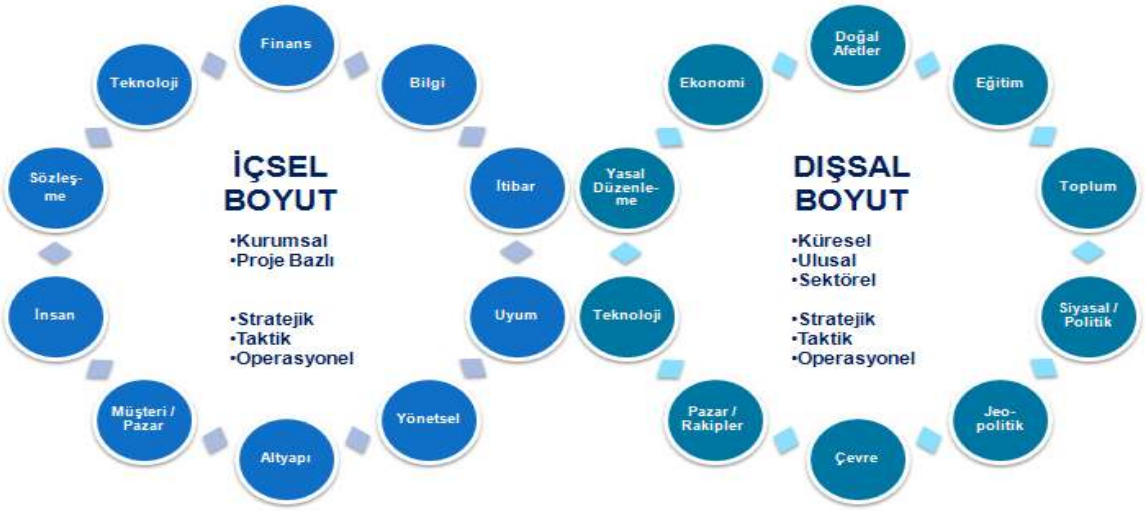
Uluslararası literatürde risk hem tehdit hem de fırsat olarak tanımlanmıştır. Bir görüş riski, global iş çevresinde faaliyette olan her organizasyonun belirsizliğe bağlantılı olarak etkilendiği zararın meydana gelme durumu şeklinde negatif bir şekilde tanımlarken (EWF, 2008), bir başka görüş, riski, bir olayın gerçekleşme olasılığı ile pozitif ve negatif etkilerinin bir birleşimi olarak tanımlamaktadır (FERMA, 2002). Bütün tanımların ortak noktası riskin geleceğe ve belli bir olasılığa yani belirsizliğe bağlı olmasıdır. Riskin geleceğe bağlı olması yönetilebileceğini gösterirken, iyi bir risk yönetimi ise risklerin tanımı, oluşma olasılığı ve alınacak aksiyonların tanımına bağlıdır. Bir başka değişle risk, bir organizasyonun belirtmiş olduğu amaçlara ulaşabilme yolunda ki belirsizlik olarak açıklanırsa,, bu belirsizlikler şirketin iş akışını ve durumunu negatif yönde etkileyebilecek ilerlemeler olabileceği gibi, fırsatlar oluşturma potansiyeline de sahip olabilir.. Risklerin işletmeyi nasıl edeceği işletmenin amaçlarına bağlı olarak değişmekte, bir işletme için tehdit oluştururken bir diğeri için de fırsat olabilmektedir (Kaşıkçı,2006)



Şekil 1. Risk Üçgeni

Kaynak: KÖKSAL A. G., *6102 Sayılı Türk Ticaret Kanunu Kapsamında Risklerin Tespiti Ve Yönetilmesin., e İlişkin Bağımsız Denetçinin Sorumluluğu,* C.Ü. İktisadi ve İdari Bilimler Dergisi, Cilt 14, Sayı 2, 2013.

Her ne kadar risk tanımı belirsizlik kavramı ile yapılsa da riski yönetimi sonucu riski belirsizlikten ayırıp belli bir istatistiki analizle hesaplanabilen ve böylece yönetilebilen belirgin bir unsur haline getire biliniyor. Bu bağlamda, risk istatistiksel olaylar, bir başka değişle geçmiş gözlemlere bağlı olarak olma olasılığının çıkarılabileceği, yenilenebilen olaylar olarak tanımlanırken, belirsizlik ise istatistiksel olmayan olaylar şeklinde tanımlanmaktadır. Dolayısıyla şirketin karşılaştığı olaylar, belli bir olasılık dağılımına göre modellenebiliyor ve alternatif sonuçları istatistiki bir şekilde hesaplanabiliyorsa risk olarak tanımlanıp yönetilebilir. Herhangi bir istatistiki modele uymadığı için yönetilemeyen olaylar belirsizliği oluşturmaktadır. (Emhan, 2009).



Şekil 2. Şirketlerde İçsel ve Dışsal Boyut

Kaynak: MERİT RİSK YÖNETİMİ VE DANIŞMANLIK, *Kurumsal Risk Yönetimi ve Uygulaması,* İstanbul 2012.

Şirketler faaliyetlerini sürdürürken hem içsel boyut hem de dışsal boyut olarak nitelendirebilecek iç içe geçmiş iki çevreden etkilenmektedir. Bir başka şekliyle şirketlerin içsel yapısı, üretimi, yönetimi, insan kaynakları, müşteri çevresi varken aynı zamanda dışsal çevrenin içinde yer alırlar. İçsel çevreyi kendi iç politikaları ile yönlendirebilirken dışsal çevre üzerinde kısmen ya da hiç etkileri yoktur. Buna bağlı olarak risklerin tanımlaması ve alınacak tedbirler ayrılmaktadır. Şirketler içsel çevreye bağlı olan risklere karşı aktif bir yönetim izleyerek, iç politika ve yönetimle bertaraf

edilebilir veya fırsata çevrilebilirken, dışsal çevreye bağlı risklere karşı pasif bir yönetim izleyerek daha çok uyum, sigortalama, çeşitlendirme şeklinde aksiyonlar alabilirler.

İçsel ve dışsal boyut altında riskler sistematik ve sistematik olmayan riskler olarak iki gruba ayrılmaktadır. Sistematik riskler dışsal boyuttan gelen iklim, kanun ve yönetmelikler, sosyal durum, ekonomik ve politik gibi bütün işletmeleri aynı yönde etkileyen risklerdir (Babuşçu, 2005). Doğal afetler, politik riskler, ekonomik riskler, yeni ulusal veya uluslararası düzenlemeler başlıca sistematik risk kaynaklarıdır. Sistematik olmayan riskler ise içsel boyuttan gelen işletme yönetimi, iş güveliği, marka, tüketici tercihleri, gibi doğrudan işletmeyi etkileyen faktörlerden ortaya çıkan risklerdir. İşletmelerin karşı karşıya kalabilecekleri sistematik ve sistematik olmayan risk türleri Tablo 1'de özetlenmiştir.

Tablo 1. Şirketlerin Karşılaştığı Risk Türleri

Risk Türü	Tanımı
İş Riski	Yanlış tanımlanmış stratejiler, yetersiz olan kaynaklar veya farklılaşan ekonomi ve rekabet ortamı nedeniyle işletme hedeflerine ulaşamama riski.
Kredi Riski	Borçlu olanın vadesi dolmuş borcu ödeyememe riski
Ulusal Risk	Hükümet tarafından garanti edilen borçların geri ödenmeme durumu riski. Günümüzde kamu yatırımları yap-işlet-devret şeklinde yapıldığı için gittikçe artan bir risktir.)
Piyasa Riski	Piyasa fiyatlarında meydana gelen değişikliklerden kaynaklanan risk
Likidite Riski	Mevcut fonların eksikliği sebebiyle vadesi dolmuş borçların karşılanamama risk
Operasyonel Risk	Dolandırıcılık faaliyetleri de dahil olmak üzere operasyonel etkiye sahip kişiler, süreç, altyapı, teknoloji vb. nedenlerle kayba uğrama riski
Muhasebe Riski	Bir organizasyonun finansal durumunu gerçeğe tam olarak yansıtmayan finansal kayıtların yapılması riski
Ülke Riski	Ülkelerarası kredi işlerinde, kredi kullanan şirketin döviz eksikliği veya iş yaptığı ülkenin ekonomik, sosyal ve politik yapısı sebebiyle sorumluluklarını yerine getirememe riski
Politik Risk	Ülkelerin mevcut politikalarından ortaya çıkabilecek risk
Endüstri Riski	Belirli bir endüstride faaliyet göstermeye bağlı oluşan risk
Çevre Riski	Kurumun kendisi veya diğer kurumlar tarafından ortaya çıkabilecek çevresel zararlar sebebiyle kayba uğrama riski
Yasal Uygunluk Riski	Yasal ve düzenleyici yükümlülüklere uymama sebebiyle risk
İtibar Riski	Bir organizasyonun itibarının zedelenmesi sebebiyle oluşan risklerdir

Kaynak: OLSSON, C., *Risk Management in Emerging Markets,* Pearson Education Limited, UK., 2002.

İş dünyasında risklerin sürekli bir şekilde belirlenmesi, sınıflandırılması, ölçülmesi, bütün ilgili birim ve yöneticilerin gerekli ve tam bilgiye ulaşmasını sağlayan şirket içi tam bilgi akışı (şirket içi düzenli raporlama sistemi) ve risk-getiri arasındaki ilişkinin anlaşılması ve optimize edilmesi, şirketin güçlenmesini sağlamaktadır. Özellikle risklerin belirlenmesi çok önemlidir, zira bu aşamada göz ardı edilen ya da gözden kaçan bir risk firmayı çok zor durumda bırakabilir. Risklerin belirlenmesinden sonra türlerine göre (tablo1) sınıflanması nispeten daha kolaydır. Risklerin ölçülmesi yani sayısallaştırılması ise en teknik kısmıdır ve her zaman mümkün olmayabilir. Örneğin ürünlerinizin hatalı olması neticesinde maruz kalabilecek olan itibar riski bulunması zor olan derin bir piyasa verisi taraması gerektirir ve kolay sarılaştırılabilen bir risk değildir (Küçüközmen, 2012)

1.2. Kurumsal Risk Yönetimin Paydaşları: Kurumsal Yönetim ve İç Denetim

Kurumsal risk yönetiminin en önemli amacı, yönetim kurulu ve ortakların iş düzenini etkileyebilecek mevcut ve olağan riskler ve fırsatlar konusunda farkındalıklarını yükseltmeyi amaçlamaktadır. Bu da kurumsal yönetim (corporate governance) ilkeleri ve iç denetim ile olabilir. Böylece karar alıcılar riskleri en iyi biçimde yöneterek organizasyonun olumsuz etkilerden en küçük zarar göreceği olumlu etkilerden daha fazla yarar sağlayacağı biçimde gerekli aksiyonları alabilirler.

Diğer bir değişle kurumsal risk yönetimi için iki ana paydaşa ihtiyaç vardır; kurumsal yönetim ve iç denetim. Kurumsal yönetim ve iç denetim 2001 yılında yaşanan kriz sonrası kanun düzenlemelerinde yer almak ile birlikte en son düzenleme kurumsal yönetimde 2011 yılında yayınlanan Serbest Piyasa Kurulu (SPK) tebliği ile iç denetim ise aynı zamanda finans dışı şirketler için ilk defa risk yönetimini getiren ve yine 2011 yılında yayınlanan Türk Ticaret Kanunu (TTK) ile olmuştur. Kanun koyucu tarafından yayınlanan kanun ve yönetmeliklerden de belli olduğu gibi iç denetim (veya iç kontrol mekanizmaları) ve kurumsal yönetim entegre bir risk yönetiminin vazgeçilmez paydaşlarıdır. Hatta yeni TTK'da risk yönetimi komitesinin kurulması ve risk yönetimi mekanizmasının çalıştırılması iç denetim komitesine bağlanmıştır. Daha sonraki bölümde bu konuda daha detaylı bilgi verilecektir. OECD tarafından 2004 yılında

yayınlanan kurumsal yönetim ilkeleri SPK yönetmelikleri ile Türkiye şartlarına uydurulmuştur ve halka açık şirketlerde zorunludur.

1.2.1. Kurumsal Yönetim

Kurumsal Yönetim (corporate governance): En geniş anlamda modern yaşamda insanların bir amaca ulaşmak için oluşturduğu herhangi bir kurumun yönetiminin düzenlenmesidir. Daha dar anlamda ise, bir kurumun toplumsal hedefler doğrultusunda kendi hedeflerine ulaşmasına ve ortaklarına ekonomik değer yaratmasına imkan tanıyan her türlü kanun, yönetmelik, kod ve uygulamaları ifade etmektedir. Kurumsal yönetimin ana ilkeleri adillik, hesap verebilirlik, şeffaflık ve sorumluluktur (TÜSİAD, 2002). OECD tarafından yayınlanan ve üye ülkelerde uygulanması zorunlu olan kurumsal yönetim ilkeleri beş alanı kapsamaktadır:

I. Hissedarların hakları;
II. Hissedarların adil muamele görmesi;
III. Doğrudan çıkar sahibi olan kesimlerin rolü;
IV. Kamuoyuna açıklama yapma ve şeffaflık;
V. Yönetim kurulunun sorumlulukları.

Kurumsal yönetim etik kurallar, kanunlara uyma, çevrenin korunması gibi bir dizi alanla örtüşen genel bir yaklaşımdır. Şirket yapısını, kültürü, stratejisi, değerleri, iş süreçleri şirketten şirkete değişiklik göstermesi nedeniyle, bu kurumsal yönetim ilkelerinin uygulamaları, ana ilkelerden ödün vermemek koşuluyla kurumların kendi ihtiyaçları doğrultusunda şekillenmelidir. Kurumsal yönetim uygulamalar ve deneyimlerle öğrenilen bir süreç olduğu için Türkiye'de kurumsal yönetim ancak zaman içinde gelişmekte, uygulamada benimsenen ilkeler bir süre sonra yasal düzenlemelere girerek zorlayıcı olabilmektedir.

1.2.2. İç Denetim

İç denetim bir şirketin operasyonlarına ilişkin belirli kurallar koyarak iş yapma prosedürlerinin oluşturulması için gereklidir. Tüm şirket personelince benimsenecek ve tüm şirket varlık ve çıkarlarını koruyacak olan iç kontrol prosedürleri bir parçasıdır. Dolayısıyla iç denetim sadece finansal varlıkların ve muhasebe sisteminin denetimi

(audit) değil bütün şirket içi prosedürlerin denetimidir. (İç Denetim Yönetmeliği, 2013). İç denetim şirketin operasyonel yapısının entegre bir parçası olarak kurulduğu zaman etkili olur ve dört ana ilkeye hizmet eder:

I. Yönetim kademesinin güvenebileceği doğru veri akışının sağlanarak karar mekanizmasının etkin hale getirilmesi,
II. Şirket içi varlık ve kayıtların çalınmasını, kaydedilmesini, kazara imha edilmesini ya da yanlış kullanımın engellenmesi,
III. Şirket içi prosedürlerin tüm süreçlerde uygulanması,
IV. Yasal zorunlulukların yerine getirilmesinin sağlanması.

Denetim komitesi ve iç denetim müdürlüğünden oluşan, iç denetim sistemi içine aynı zamanda riskli alanları belirlenmesi sürecinde eklenmiş olsa da iç denetim belirleyeceği risklerin yönetimi için risk yönetimi komitesine ihtiyaç vardır. Ayrıca iç kontrol sisteminde insan faktörü olduğu için insani hataların olasılığı hep göz önünde tutulmalıdır.

1.3. Kurumsal Risk Yönetimi Nedir ve Neden Önemlidir

Kurumsal Risk Yönetimi, şirketin içsel ve dışsal çevreye ait risklerin belirlenip, yönetilebilir yani geçmişe yönelik datalar (bilgiler) yardımıyla istatistiki bir şekilde sayısallaştırılabilir risklerin yönetilmesi, daha çok dışsal çevreden gelen ve istatistiki olarak sayısallaştırılamayan risklerin sigortalama veya taşerona devretme gibi aksiyonlar alarak transfer edilmesi amacıyla, şirket kültürüne bağlı olarak risk yönetimi sistemi oluşturulup hayata geçirilmesi olarak özetlenebilir.

İlk çıkış noktası Türkiye'de de ISO standartları ile bilinen kalite kontrol sistemleridir. En başta kalite kontrol sistemleri üretim sektöründe üretimin kaliteli olması için kullanılıp, ürün bazlı sertifika verilirken daha sonra hizmet sektörüne de uygulanmış ve şirketlere topyekûn ISO sertifikası verilmeye başlamıştır. Kısaca her yapılan işlemin tanımının yapılması ve gelişmiş bir raporlama sistemi olarak tanımlanabilecek kalite kontrol mekanizmalarında, sertifika veren kuruluşlar tarafından sürekli denetlenerek uygulamanın sürekliliği sağlanmaktadır. Fakat ortaya çıkan daha çok finansal bazlı skandallar bu uygulamanın yeterli olmadığını göstererek örgüt

kültürünü değiştirecek kurumsal yönetim ilkelerinin çıkmasına neden olmuştur. Kurumsal yönetim ile şirket üst yönetiminde etik olgu oluşturulmaya çalışılmış, yönetimin şeffaflık, adillik ve hesap verilebilirlik ilkelerine göre şekillenmesi için gerekli raporlama ve organizasyonel şekillenme ön görülmüştür. Daha sonra yeni TTK ile zorunlu tutulan iç denetim mekanizması ile kurumsal risk yönetiminin alt yapısı hazırlanmıştır. Bununla birlikte gelişmiş bir şirket kültürünün bir parçası olan entegre bir kurumsal risk yönetimi sistemi henüz ülkemizde tam olarak uygulandığı söylenemez.

Tablo 2. Risklere Ait Geleneksel ve Yeni Bakış

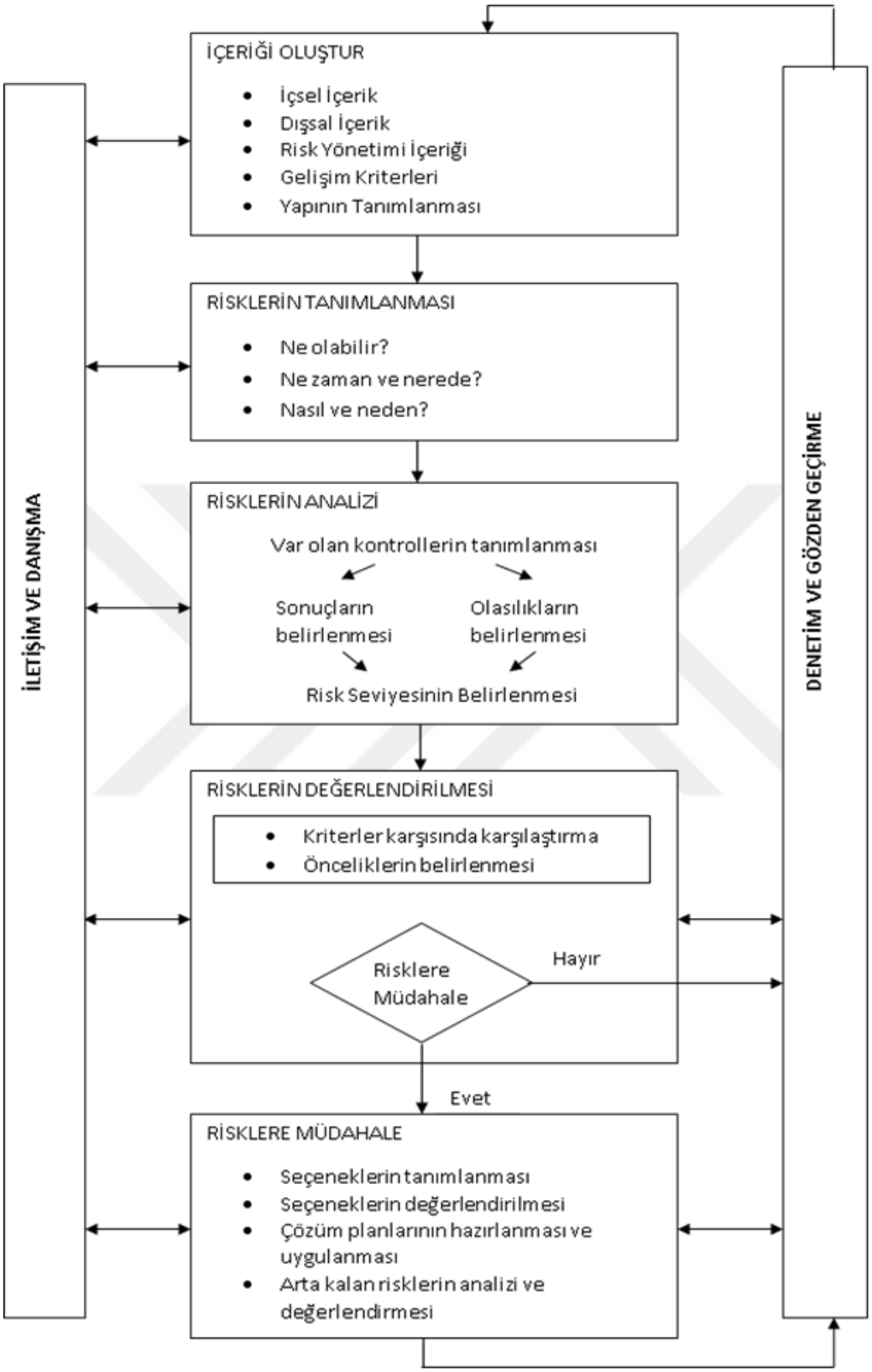
Geleneksel Görüş	**Yeni Görüş**
Risk kontrol edilmesi gereken olumsuz bir faktördür.	Risk bir fırsattır.
Risk üretim ve proje bazlı yönetilir.	Risk bir bütün olarak şirket çapında yönetilir.
Risk yönetiminin sorumluluğu aşağı seviyelere delege edilir.	Risk yönetiminin sorumluluğu üst yönetim ve kısım yönetimleri tarafından kabul edilir.
Risk ölçümü sübjektiftir.	Risk objektif bir şekilde ölçülebilir.
Yapılanmamış ve tutarsız risk yönetim fonksiyonları bulunur.	Risk yönetimi bir bütün olarak kurulup şirket yönetim sistemlerine entegre edilir.
Yönetim Kurulunun iç kontrolünü sağlayan bir denetleme komitesi vardır.	Yönetim Kurulunun etkili risk yönetimi yapısını sağlayan bir risk yönetimi komitesi vardır.

Kaynak: PRİCEWATERHOUSECOOPERS, *Her Yönüyle Kurumsal Risk Yönetimi*, PWC, Infomag Yayıncılık, 2006.

Kurumsal risk yönetimi, gereksinim duyduğu topyekün bir sistemin parçası olan raporlama, denetim ve organizasyonel yapılanma sayesinde, kurumsal yönetimin ana ilkelerinden olan farkındalık ve şeffaflık konularının bütün şirket uygulamalarına geçmesini sağlar, bu suretle yatırımcı ve diğer paydaşlar tarafında "Kurum" algısını da güçlendirmektedir. Entegre bir sistem olarak düşünülmesi gereken kurumsal risk yönetimi, kurumsal yönetim ilkeleri ışığında oluşturulan ve şirket içi mükemmel bilgi akışını sağlayan işlem bazlı ve finansal raporlama ve iç denetim ayakları üzerine kurulmalıdır.

Şekil 3'de iş akışında da görüldüğü gibi risk yönetimi iletişim ve danışma yani raporlama ve denetim ve gözden geçirme yani geri bildirim ana çerçevesi içeresinde şekillenmektedir. Raporlama, risklerin sınıflandırılarak sarılaştırılabilmesi için gerekli bilgiyi sağlarken, iç denetim bu bilgilerin gözden kaçmasını engellemektedir. Risk yönetiminde risklerin belirlenmesi kadar, risklerin değerlendirilmesi ve gerekli müdahalelerin (aksiyonların) belirlenmesi ve bu aksiyonların uygulamaya konulmasını rutinleştiren bir mekanizmanın oluşturulması da çok önemlidir. Böylece risk yönetimi, yönetim kurullarının, icraya bağlı gözetim sorumluluklarını yerine getirebilmesine yardımcı olabildiği gibi, paydaşlarına ve diğer çıkar sahiplerine de organizasyonun yasal düzenlemelere ve kurumsal yönetim prensiplerine göre yönetildiğine dair güvence sağlar.

Rekabet ortamıyla başa çıkmak, değişen piyasa koşullarına hızlı bir şekilde cevap vermek ve fark yaratmak, örgüt kültürünün aile şirketi yapısından çıkıp kurumsallaşması ve kurumsal risk yönetimi sistemi oluşturularak uygulanması ile mümkündür. Özellikle finans dışı sektör, finansman için finans sektörüne bağımlı olmakla birlikte, finansa sektöründen ayrı olarak üretim yaparak veya hizmet vererek para kazanma amacıyla faaliyet gösterdiği için daha fazla riske maruz kalmaktadır. Bununla birlikte finans dışı şirketlerde -büyüklüklerine göre-, risklerini belirlemede ve ölçmede, gerek teknik altyapı gerekse uzman personel açısından oldukça yetersizdir. Bu yüzden özellikle küçük ölçekli şirketler finansal piyasalarda meydana gelen en küçük bir değişimden ya da belirsizlikten hemen etkilenmekte ve bu etkilerden korunamamaktadırlar (Topçu, 2010).



Şekil 3. Entegre Kurumsal Risk Yönetimi Sistemi

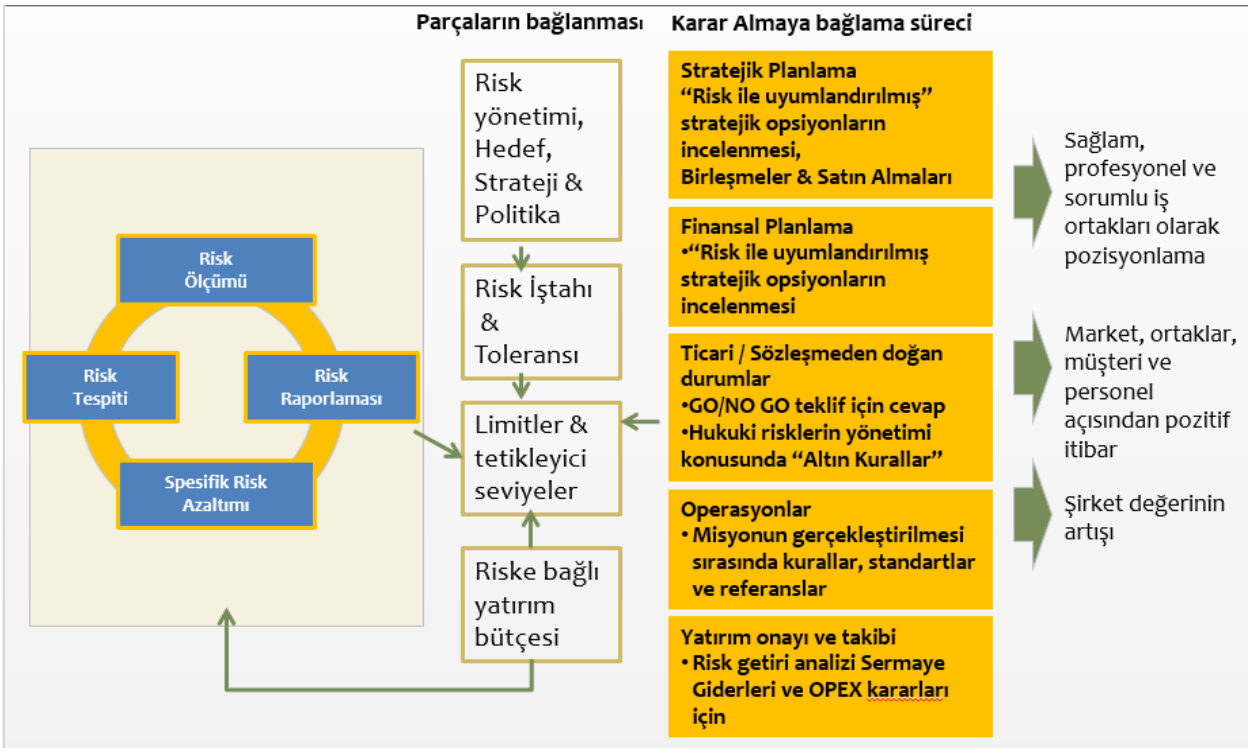
Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004

Halka açık şirketlerde uygulanması zorunlu kurumsal yönetim ilkeleri ve yeni TTK düzenlemesi ile getirilen ve iç denetim mekanizmasına bağlanan risk yönetimi ışığında, iyi ve ilerletilebilir bir büyüme amaçlayan ve geçirilen krizlerden ders alıp gereken önlemleri alma ihtiyacının farkındalığı ile hareket eden şirketler sürekli bir risk yönetimi stratejisi geliştirebilmek için kaynak oluşturmaktadır. Fakat bu bilincin kaynak kıtlığından ve organizasyonel kültürden dolayı daha çok halka açık büyük şirketlerde görebilmekteyiz. Büyük şirketlerin fason üreticisi olarak çalışan küçük şirketler de büyük şirketlerin yardımıyla kalite kontrol mekanizmasının gerektirdiği raporlamalar yapmaktadırlar. Maalesef ülke ekonomisinde önemli bir yer tutan inşaat sektöründe ise büyük ve eski inşaat firmaları dışında herhangi bir risk yönetimi veya paydaşlarından olan kurumsal yönetim ve iç denetim uygulanmamaktadır. Hatta risk yönetiminin ilk dayanağı sayılan kalite kontrol mekanizmaları bile tam olarak oluşturulmamıştır.

Etkin bir risk değerlendirme ve yönetim sistemi ile karmaşık hale gelen süreçler, değişen koşullar, artan belirsizlik ortamı, ekonomik ve politik dalgalanmalar karşısında organizasyonun daha dirençli hale gelmesi sağlanabilir. Bu bağlamda, Kurumsal Risk Yönetimi üzerine AICPA (Uluslararası muhasebeciler sertifika derneği) ve NC STATE UNIVERSITY'nin 2011 yılında 700'den fazla kurumu temel alarak yaptığı ankete göre, ankete katılan üst düzey yönetim ve şirket çalışanlarının %60'ından fazlası son 5 senede piyasa ve kurumsal risklerin büyük bir artışa geçtiğini düşünüyor. Katılımcılardan %59'u risk yönetimi uygulamasının içselleştirilmesinin şirket yönetimine oldukça pozitif katkısı olduğunu ve böylece karlılık oranlarını artırdıklarını belirtmiştir.

Riskler, aktivitelerin içindeki önemli bölümler olup, işlem süresince düzgün ve bütünsel olarak yönetilmeleri gerekir. Dolayısıyla, risk yönetimi, herhangi bir aktivite, fonksiyon ve işlemle ilgili belirleyici, analiz edici, uygulayıcı, çalıştırıcı ve riskler arasında ilişki kurucu, mantıklı ve sistematik bir metodudur. Aynı zamanda şirketlerin zararlarını minimize edip, fırsatlarını maksimize etmeye yönelik bir sistemdir. Risk yönetimi şirketin bütün operasyonlarını ve bütün süreçlerini kapsadığı için tem yekün şirketin bütün yönetim sistemine entegre edilmesi gerekmektedir.

Organizasyon içi görevlerin çalışanları becerileri ve işlerin gereksinimlerine göre bilinçli oluşturulması, iş yapış yolları için en uygun uygulamaların örnek alınması, faaliyetlerden en yüksek yarar sağlanabilmek için organizasyon içinde görüşülmesi, belgelendirilmesi ve bu şekilde kurumsal oluşumun sağlamlaştırılması, risk yönetimi işlevinin öncelikli amaçları arasındadır. Risk yönetimi oluşum aşamasının iyi oluşturulmuş olmasının yanında, bu sistemin işleyen bir yönetim yolu olabilmesi için yalın ve değiştirilebilir bir oluşuma sahip olmasında büyük yarar vardır. Şirketin ölçeği ve ihtiyaçlarına göre bir risk komitesi oluşturulmalıdır.



Şekil 4. Risk Yönetiminin Şirket Operasyonlarına Entegre Edilmesi

Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004.

Kurumsal risk yönetimi içeresinde yönetim kuruluna bağlı olarak görev yapacak risk komitesinin hedefi, şirketin maruz kalabileceği risklerin gözlemlenmesi ve risk yönetimi aşamalarının devam ettirilebilir olabilmesi için gerekli politikaların geliştirilmesidir. Bu birimlerde görev yapacak kişilerin, muhasebe, finans, denetim, hukuk, yönetim vb. bölümlerde iş tecrübesine sahip uzman bireyler olması önerilir. Aktif risk yönetimi sistemi, iç kontrol sisteminin gelişmesine faydalı olabileceği gibi, iç denetim bölümünün etkinlikleri için de önemli bir durum teşkil eder. İç denetim bölümü, etkinliklerini oluştururken, risk yönetim sisteminin etkinliğini de değerlendirmelidir.

Kısaca özetlersek, entegre kurumsal risk yönetimi fonksiyonları şu şekilde işler:

I. Organizasyonun hedeflerine yönelik finansal, operasyonel, stratejik, hukuksal, dış riskler ve itibar riskleri belirlenir.
II. Kilit Risk İndikatörleri (KRI) belirlenir; risk izleme araçlarından yararlanılarak risklerin takibi yapılır.
III. Organizasyonel hedefler göz önünde bulundurularak risklerin potansiyel etkileri için limitler atanır.
IV. Limitlerin aşılması durumunda hızla aksiyon almak üzere aksiyon planları hazırlanır, sorumluluklar paylaştırılır, sorumlular ile düzenli iletişim sağlanır.
V. Periyodik risk raporları ve risk komiteleri ile yönetim kurulu bilgilendirilir.

Bütün bu işlemlerin düzgün yapılabilmesi için bir risk komitesi kurulması ve şirket yönetimsel yapısının risk yönetimin ihtiyaçlarına göre değiştirilmesi gerekmektedir. Risk yönetimi sadece riskin düşürülmesi ya da kontrol edilmesine yönelik bir tutum değildir. Eğer risk yönetimi şirket işleyişine bütünüyle entegre edilmez ve sadece finansal raporlama ve denetimi olarak görülürse risk yönetiminden fayda sağlayamaz. Entegre risk yönetimi sistemi risklerden doğacak zararları en az indirerek olası fırsatları değerlendirmeyi mümkün kılarak, getiri ve sermaye arasında optimal uyum sağlamaktadır (Olsson, 2002).

Şekil 5. Kurumsal Risk Yönetimi Kapasitesi

Kaynak: MERİT RİSK YÖNETİMİ VE DANIŞMANLIK, *Kurumsal Risk Yönetimi ve Uygulaması,* İstanbul 2012.

Risk yönetimi ancak şirket içi veya dışı eğitim ile uygulaması geliştirilip şirket kültürü haline getirilebilir. Piyasa koşulları, iş ortamı, ihtiyaçlar sürekli olarak değiştiği için, risk yönetiminde sürekli değişmesi gerekiyor ve bu duruma personelin adapte olabilmesi için sürekli eğitim verilmesi gereklidir, dolayısıyla risk yönetiminin durağan olması düşünülemez. Risk yönetiminin riskleri azaltma bakış açısından çıkarılıp, fırsat yönetimi haline getirebilmek için sürecin her kademesi belli bir öğrenme, araştırma, hesaplama ve uygulama evresini içermelidir (Küçüközmen, 2012).

2. TÜRK TİCARET KANUNU VE YÖNETMELİKLER'İN KURUMSAL RİSK YÖNETİMİNE YAKLAŞIMI

2.1. Türk Ticaret Kanunu'nun Risk Yönetimine Bakışı

Risk yönetimi kavramı, 6102 sayılı Türk Ticaret Kanunu'nda yer alan düzenlemelerle birlikte 13 Ocak 2011'de TBMM'nde kabul edilerek 14 Şubat 2011 tarihinde Resmi Gazete 'de yayınlanarak, ticaret hukukumuza ilk kez girmiştir. Ancak Kanun henüz yürürlüğe girmeden 50 maddesinde 6335 sayılı Kanun ile değişiklik yapılmış ve 1 Temmuz 2012 tarihinde yürürlüğe girmiştir. Risk yönetimi ile ilgili düzenlemeler yönetim kurulunun görev ve tetkikleri başlığı altında bulunana maddelerin içinde yer almıştır.

6102 sayılı TTK kanunun 366. maddesinde anonim şirketlerde "iç denetim" amacıyla komisyon kurula bileceğinden bahsedilmektedir. 367. maddede iç kontrol sisteminin ana dayanağı olan şirket içi yönergenin tarifi yapılmıştır. Kanuna göre iç yönerge: "Şirketin yönetimini düzenler; bunun için gerekli olan görevleri tanımlar, yerlerini gösterir, özellikle kimin kime bağlı ve bilgi sunmakla yükümlü olduğunu belirler". 375. maddede yönetim kurulunun devredilemez ve vazgeçilemez görev ve yetkileri arasına "finansal planlama", kontrol mekanizması olarak "üst gözetim", "kurumsal yönetim" kavramları sokularak risk yönetimi mekanizmasının kurulabilmesi için gerekli alt yapı belirlemektedir. Bu bağlamda kanuna göre: "Muhasebe, finans denetimi ve şirketin yönetiminin gerektirdiği ölçüde, finansal planlama için gerekli düzenin kurulması; Yönetimle görevli kişilerin, özellikle kanunlara, esas sözleşmeye, iç yönergelere ve yönetim kurulunun yazılı talimatlarına uygun hareket edip etmediklerinin üst gözetimi; Pay, yönetim kurulu karar ve genel kurul toplantı ve müzakere defterlerinin tutulması, yıllık faaliyet raporunun ve kurumsal yönetim açıklamasının düzenlenmesi ve genel kurula sunulması, genel kurul toplantılarının hazırlanması ve genel kurul kararlarının yürütülmesi" zorunludur.

Risk yönetimi açısından en açık madde yönetim kurulunun görev ve yetkileri içeresindeki riskin erken belirlenmesi ve yönetimi başlığı altında yer alan 378. maddedir. Maddede yer alan "erken teşhis", "tehlike", "önlemler ve çareler", "riskin

yönetilmesi", "risk komitesi", "risk raporu" gibi kavramlar aracılıyla kurumsal risk yönetimi mekanizması oluşturulması şartlandırılmıştır.

"MADDE 378 -(1) Pay senetleri borsada işlem gören şirketlerde, yönetim kurulu, şirketin varlığını, gelişmesini ve devamını **tehlikeye** düşüren sebeplerin **erken teşhisi,** bunun için gerekli **önlemler ile çarelerin** uygulanması ve **riskin yönetilmesi** amacıyla, **uzman bir komite kurmak**, sistemi çalıştırmak ve geliştirmekle yükümlüdür. Diğer şirketlerde bu komite denetçinin gerekli görüp bunu yönetim kuruluna yazılı olarak bildirmesi hâlinde derhâl kurulur ve ilk **raporunu** kurulmasını izleyen bir ayın sonunda verir.

(2) Komite, yönetim kuruluna her iki ayda bir vereceği raporda durumu değerlendirir, varsa tehlikelere işaret eder, çareleri gösterir. Rapor denetçiye de yollanır."

Bu maddede tüm anonim şirketler için öngörülmüş bulunan finans denetim ve denetim komitesi yanında bir diğer iç kontrol mekanizmasını vurgulanmaktadır. Bu komitenin denetim komitesinden farkı denetim komitesinin yönetimi gözetim altında tutmasına karşılık bu komitenin sadece risklere odaklanmasıdır. Ayrıca denetim geçmişe yönelik bir inceleme olmasına karşılık, risklerin belirlenmesi gelecek ve geleceğin yorumuyla ilgilidir. Denetimin yönetilmesi söz konusu olmadığı halde, tehlike olarak kanunda yer bulan riskler, yine kanunda yer alan önlemler ve çareler çerçevesinde yönetilebilir. Amaç, yönetimi, yönetim kurulunu ve genel kurulu devamlı risklerden haberdar etmek ve gereğinde organlarca derhal etkili önlemlerin alınmasını sağlamaktır. Bu sebeple komite sorumluluk sisteminin merkezinde yer alır.

Kanun erken uyarı sistemine istisnaî bir önem verdiğinden bu konuda denetçileri de özel olarak görevlendirmiştir. Bu önem 398, 402 ve 403. Maddelerde yer alan deneticinin görevlerinde de anlaşılmaktadır. Özellikle madde 398'de "denetçi, yönetim kurulunun şirketi tehdit eden veya edebilecek nitelikteki riskleri zamanında teşhis edebilmek ve risk yönetimini gerçekleştirebilmek için 378. maddede öngörülen sistemi ve yetkili komiteyi kurup kurmadığını, böyle bir sistem varsa bunun yapısı ile komitenin uygulamalarını açıklayan, ayrı bir rapor düzenleyerek, denetim raporuyla birlikte, yönetim kuruluna sunar" risk yönetiminin oluşturulması şirket denetiminin içinde yer almıştır.

Tehlikelerin erken teşhisi ve önlenmesi için gerekli olan risk komitesi, bazı yönetim kurulu üyelerinin görev vermeleri durumuyla kurulabileceği gibi, tamamen üçüncü şahıslardan da oluşabilir. Denetleyeni bir başka mühim görevi de gereklilik ortaya çıktığı durumda komitenin oluşturulması, hisse senetleri borsada işlem görmeyen bir şirketten de istemesidir.

2.2. Yeni Türk Ticaret Kanunun Öngördüğü Risk Yönetimi Uygulaması

Türk Ticaret kanununun risk yönetimine ilişkin maddeleri genellikle organizasyonel yapı ve iç denetim unsurlarını ön plana çıkarmak ile birlikte risk yönetimini nasıl yapılması gerektiğine ilişkin bir yöntem ya da ayrıntı vermemektedir.

Öncelikle riskleri zamanında teşhis edebilmek ve risk yönetimini gerçekleştirebilmek için öngörülen sistem kurumsal risk yönetiminin gerektirdiği bir sistemden ziyade bir erken uyarı sistemi olarak ele alınmaktadır. Kurumsal risk yönetimi iç içe geçmiş karmaşık ve uzmanlık gerektiren süreçler topluluğu olup, maruz kalınacak risklerin belirlenmesi, tanımlanması, sınıflanması, ölçülebilir hale getirilmesi ve nihayetinde yönetilmesi aşamaları içermektedir. Dolayısıyla gerçek zamanlı güncel veri ve bunun analizi üzerine kurulmuştur. Bu açıdan özellikle pay senetleri BİST'de işlem gören halka açık şirketlerde, şirketin maruz kalabileceği risklerin erken teşhisi için uzman bir komitenin kurulması, çalıştırılması ve geliştirilmesine ilişkin esaslar ve hatta zorunlu tutulması için idari yaptırım ayrıca ve kapsamlı olarak ele alınmalıdır. Konuya sadece düzenleme açısından bakmak ya da düzenlemeye uyum için komiteler kurma çabaları maalesef gittikçe karmaşıklaşan risklere karşı belirgin bir koruma sağlamayacaktır. Son aylarda görülen döviz dalgalanması sonucu reel sektörde oluşan aşırı borç yükü krizi ve konkordato ilanları bunun açık bir göstergesidir.

2.3. İş Sağlığı ve Güvenliği Kanunu ve Uygulaması

Gerek ülke ihtiyaçları, gerek Avrupa Birliği ve uluslararası taahhütler doğrultusunda, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu 30 Haziran 2012 tarihinde yürürlüğe girmiştir. Kanun ile birlikte çıkan yönetmeliklerde koruyucu ve iyileştirici bir anlayış benimsenmiştir. Bu kanun ile risk değerlendirilmesi daha çok işin fiziki yapılma

koşullarına ve şekline yönelik olup iş sağlığı ve güvenliği profesyonellerinin çalıştırılması iş kolundaki tehlike sıralamasına göre zorunlu hale getirilmiştir.

Uygulamadaki zorluklar ve ülke ihtiyaçları doğrultusunda 3 kez önemli değişiklikler yapılarak kanunun uygulanmasına yönelik etkinlik artırılmıştır. En son 18 Haziran 2017 tarihli ve 7033 sayılı kanunla yapılan değişiklik sonucu, "50'den az çalışanı bulunan ve az tehlikeli sınıfta yer alan iş yerlerinde; (işe giriş, periyodik muayeneler ve tetkikler hariç) iş sağlığı ve güvenliği hizmetleri, işverenler veya işveren vekilleri tarafından (İş sağlığı ve güveliği sertifikası olması şartıyla) yürütülebilecek. 50'den az çalışanı olan ve az tehlikeli sınıfta yer alan iş yerleri de (işyeri hekimleri yerine) aile hekimleri ve kamu sağlık hizmeti sunucularından hizmet alabilecek" hükmü getirilmiştir. Kısaca 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu'nun ile getirilen az tehlikeli sınıfta aylık sürekli hekim ve uzman görevlendirmesi hükümleri, 1 Temmuz 2017 yerine 1 Temmuz 2020'de yürürlüğe girecektir.

6331 sayılı İş Sağlığı ve Güvenliği Kanunu Kanunun getirdikleri:

I. İşyerlerine, risk değerlendirmesiyle (buradaki risk değerlendirmesi daha önce bahsedildiği gibi dar kapsamlıdır) birlikte önleyici bir iş sağlığı ve güvenliği yaklaşımı,
II. Bütün sorumluluk işyeri sahiplerine ait olarak; iş sağlığı ve güvenliğinin işyerlerinin tamamında kabullenilmesi ve uygulanması,
III. İşverenin; çalışanları ile birlikte işin her aşamasında işten kaynaklı tehlikeleri sürekli olarak tespit ederek, muhtemel risklere karşı tedbir alması,
IV. Kanun, iş sağlığı ve güvenliğinde en iyi şartları amaçlayarak, işyerinin o anki durumunun devamlı düzeltilmesi,
V. İş kazası veya meslek hastalığı olduktan sonrasında nelerin uygulanacağı değil, öncesinde önlemek için atılacak adımların belirlenmesi.

İş sağlığı ve güvenliği profesyonellerinin çalışma süreleri ve görevlendirilmesi, çalışanların iş sağlığı ve güvenliği eğitimlerinin süreleri ile acil durum planı ve risk değerlendirmesinin yenilenmesi gibi hizmetlerinin daha etkin sunumu amacıyla şirket büyüklüğünün yanında şirketin bulunduğu iş koluna göre tehlike sınıfları belirlenmiştir. Bu gruplandırmada; gerçekleştirilen asıl işin özelliği, işin her bölümünde kullanılan

veya ortaya çıkan maddeler, iş ekipmanı, üretim yöntem ve şekilleri, çalışma ortam ve şartları gibi kısımlar göz önüne alındı.

Tablo 3. İşyeri Sınıfları

İşyeri tipi	Tehlike sınıfı
0 - 10 Çalışan	Az Tehlikeli
10 - 49 Çalışan	Tehlikeli
50 ve üstü çalışan	Çok Tehlikeli

Kaynak: ÇSGB, *6331 Sayılı İş Sağlığı ve Güvenliği Kanunu,* T.C. Çalışma ve Sosyal Güvenlik Bakanlığı Genel Yayın No: 52, Ankara, 2016.

Az Tehlikeli Sınıflar: Eczaneler, Lokantalar, Oteller, Okullar, Yurtlar, Perakende Mağazalar, Marketler, Apartmanlar, Büroda hizmet verenler (avukatlar, muhasebeciler, gümrükçüler, emlakçılar, reklam ajansları…) Basit tarzda tekstil imalatı ve gıda imalat ve satış işleri vb…

I. Tehlikeli Sınıflar: Dişçiler, Kuaförler, Film Yapım Şirketleri, kasaplar, ayakkabı ve mobilya gibi bazı fabrikalar…
II. Çok Tehlikeli Sınıflar: Yapı – İnşaat Sektörü, Maden – Metal – Kimya Sanayi, Hastaneler…

İş sağlığı ve güvenliği kanunu ve ilgili yönetmeliklerle birlikte getirilen yasak zorunluluk uygulamaların yaygınlaşabilmesi için idari yaptırımlar da getirilmiştir. Bakanlıkça idari para cezalarından elde edilecek gelir, iş sağlığı ve güvenliği ile ilgili eğitim ve araştırma-geliştirme projelerine harcanacağı ve maden işyerlerinde ölümlü iş kazasının meydana gelmesi halinde işveren iki yıl süre ile kamu ihalelerinden yasaklanacağı belirtilmiştir. Kanuna aykırılığın tespiti durumunda, çalışan sayısı ve tehlike sınıfına göre idari para cezaları %25 ila %200 oranında artırılarak uygulanmaktadır.

Tablo 4. İşyeri Sınıflarına Göre İdari Cezalar

İşyeri tipi	Az Tehlikeli	Tehlikeli	Çok Tehlikeli
0-10 Çalışan	Aynı miktar	+%25	+%50
10-49 Çalışan	Aynı miktar	+%50	+%100
50 ve üstü çalışan	+%50	+%100	+%200

Kaynak: ÇSGB, *6331 Sayılı İş Sağlığı ve Güvenliği Kanunu,* T.C. Çalışma ve Sosyal Güvenlik Bakanlığı Genel Yayın No: 52, Ankara, 2016.

Özellikle tehlikeli iş kollarında operasyonlarını sürdüren şirketler belirgin standartları takip etmek, tüm seviyelerde personelini eğitmek ve tüm önlemleri almak durumundadır.

Türkiye'de yaygın bir anlayış iş sağlığı ve güveliği yönetmeliğini risk yönetimi için yeterli olarak görmektedir. Oysaki iş sağlığı ve güveliği yasası sadece kurumsal risk yönetimin fiziki olarak görebileceğimiz bir parçasıdır. Kurumsal risk yönetimi sadece fiziki riskleri değil bütün risklerin veya fırsatların değerlendirilip bir şirket felsefesi haline getiren bir yönetim anlayışıdır. Uygulaması zorunlu olan iş sağlığı ve güvenliği yönetmeliğine rağmen, 2014 yılında Soma'daki kömür madenin de yaşanan ve 301 madencinin ölümüne neden olan felaket, 3. Havalimanı yapımında resmi kaynaklara göre 27, sendikaya göre 35 işçinin ölümü, özel sektörde iş kazalarının sayılarının yıldan yıla artması ve 2016 yılında toplam 1405 kişinin hayatını kaybetmesi uygulamada önemli aksaklıkların olduğunu göstermektedir.

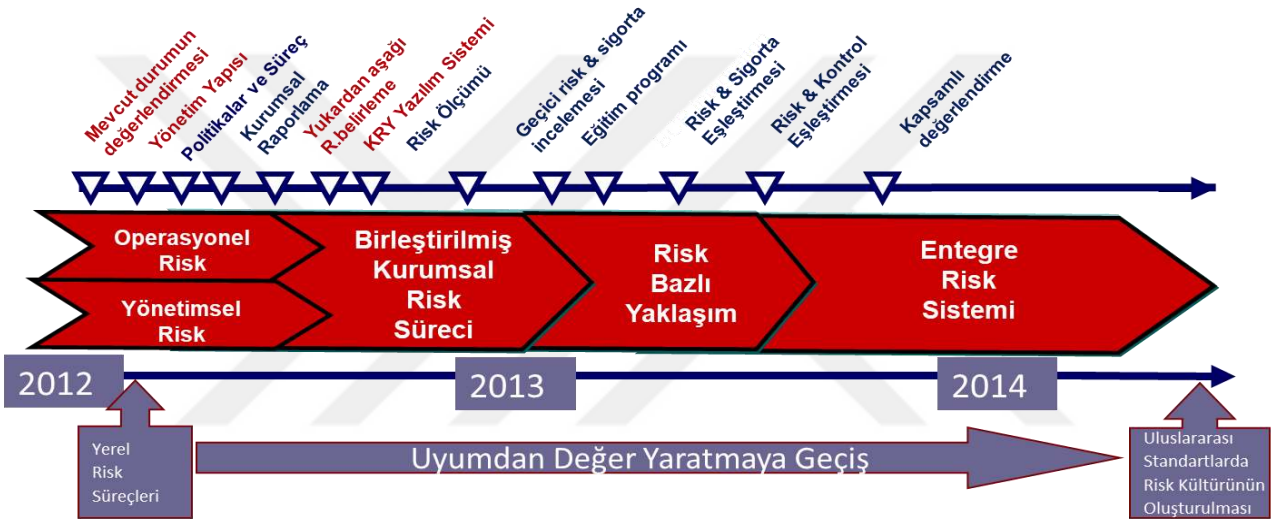
Tablo 5. Türkiye'de Meydana Gelen İş Kazaları ve Ölümler

	2011	2012	2013	2014	2015	2016
Toplam İş Kazası	69.227	74.871	191.389	221.366	241.547	286.068
Meydana Gelen Ölüm	1700	744	1360	1626	1252	1405

Kaynak: SGK, *İş Kazası ve Meslek Hastalıkları İstatistikleri,* http://www.sgk.gov.tr, 2017.

3. KURUMSAL RİSK YÖNETİMİ SÜRECİ VE METODOLOJİSİ

Dünya'da birçok ülke değişik standartlara bağlı olarak değişik kurumsal risk yönetimi uygulama modelleri bulunmaktadır. Temelde hepsi ISO 31000[1] standartları çerçevesinde geliştirilmiştir. En çok uygulanan modeller ise Avustralya ve Yeni Zelanda Risk Yönetim Modeli, İngiltere Risk Yönetim Modeli, Kanada Risk Yönetim Modeli ve Amerika Risk Yönetim Modelidir. Özellikle Kurumsal Risk Yönetimi modelleri arasından en yaygın olarak kullanılan ve bilinen model COSO tarafından oluşturulan Amerika Risk Yönetim Model'idir.



Şekil 6. Kurumsal Risk Yönetimi Uygulama Dönüşümü

Kaynak: IRM, *Kurumsal Risk Yönetimine (KRY) Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri,* AIRMIC, ALARM, IRM, 2010.

3.1. Kurumsal Risk Yönetimi Standartları

Globalleşme, artan rekabet, karmaşıklaşan finansal enstrümanlar, hassas ve oynak piyasalar ve ortaya çıkan skandallar ve krizler çerçevesinde, iç denetim, kurumsal yönetim, ve son olarak sosyal, çevre ve yönetişimi de içeren entegre risk yönetimi[2] konusundaki uluslararası yasal düzenlemeler ve standartlar kısaca; COSO Çerçevesi,

[1] 2008'deki küresel finansal kriz sonrası, 2009 yılında Uluslararası Standardizasyon Organizasyonu (ISO) 31000 standardını yayınlamıştır. Kullanım hakları İngiliz Standartlar Enstitüsüne (BSI) aittir.

[2] COSO ile Dünya Bankası 2017 yılında birlikte geliştirdikleri yeni standartlar, "Guidance for Applying Enterprise Risk Management (ERM) to Environmental, Social and Governance (ESG)-related Risks".

Avustralya-Yeni Zelanda Risk Yönetimi Standartları-AS/NZS 4360-2004, Sarbanes Oxley Act, FERMA Standartları-ISO 31000, Basel Risk Yönetimi Pratiği Kılavuzu'dan oluşmaktadır. Bu uluslararası standartlar ve yerel yasal düzenlemeler bir şirketin kendi sektörüne, aşama ve standartlarına göre bir risk çerçevesi oluşturmasına yardımcı olabilmektedir.

3.1.1. Sox - Sarbanes-Oxley Act

Enron, Xerox ve Worldcom muhasebe ve denetim skandallar sonucu ABD'de Sermaye Piyasası Kurumunun eş değeri olan Securities and Exchange Comission (SEC) tarafından, ABD sermaye piyasalarında faaliyet gösteren yerli ve yabancı firmalar için getirilmiş ve 2002 yılında yürürlüğe girmiş en önemli düzenlemedir. Bu kanun kurumsal yönetimin şirketler tarafından uygulanmasını zorlamak ve şirket şeffaflığını arttırmak amacıyla, firmaların özellikle kurumsal yönetim kadrolarına ve denetim komitelerine ciddi yükümlülükler ve yeni raporlama şartları getirmiştir. Türkiye'de de aynı skandalları yaşamamak için Sarbanes Oxley Kanununun hükümlerini 2002 yılında yayınlanan SPK'nın Seri: X No:19 Tebliği ile Türkiye'de uygulamaya geçirmiştir. Türkiye'de kurumsal yönetim konusuna yeterince değinilmediği için denetim firmalarının seçiminde bu güne kadar olduğu gibi tebliğden sonrada doğal olarak fiyat unsuru öne çıkmış, bağımsız denetimin işlevi ve yararı ortaya çıkması zorlaşmıştır (Erdikler, 2003).

3.1.2. Avustralya/Yeni Zelanda Standardı - AS/NZS 4360:2004

AS/NZS 4360 standardı 1999 da geliştirilmiş ve 2004 de güncellenmiş; risklerin entegre bir şekilde yönetilmesi ve belgelenmesinde dünyanın ilk resmi standardıdır. Bu standarda göre risk yönetimi, iyi bir firma yönetiminin tamamlayıcı bir parçası olup, ayrı bir süreç yerine mevcut uygulamalara veya iş süreçlerine en iyi şekilde uyum sağlayarak, sürekli gelişmenin en önemli parçasıdır. AS/NZS 4360 jenerik bir kılavuz olarak daha basit ve esnektir ve Sarbanes-Oxley uyumu gerektiren organizasyonlar için iyi çalışır. Bunula birlikte tehdit risk modelli metotları ele almadığı için teknik riskler için iyi çalışmaz, daha çok organizasyonel ve sistematik riskler için etkin bir risk yönetimi sağlar.

AS/NZS 4360 risk standardı beş önemli bileşen içerir:

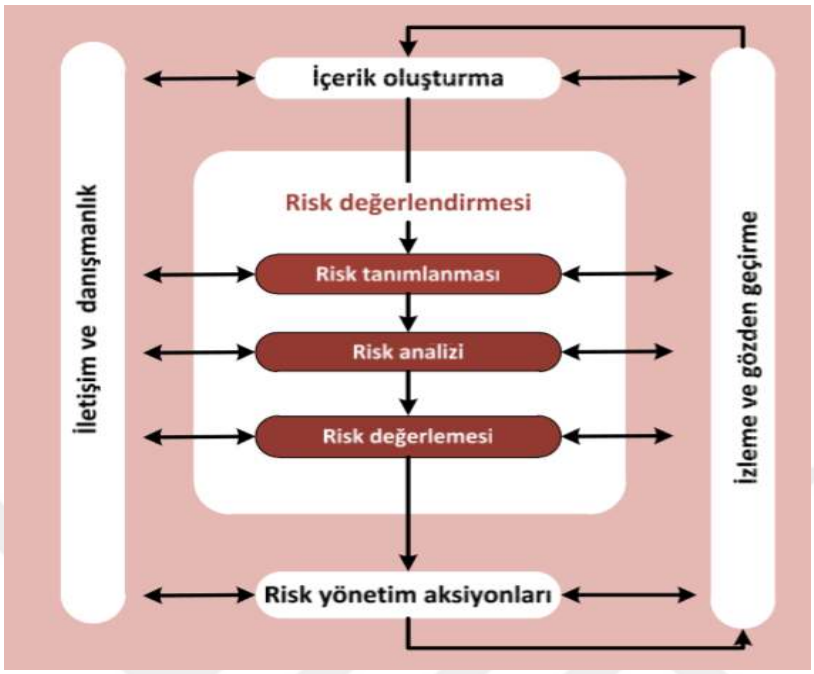
I. İçeriği saptamak: Ele alınan risklerin saptanması diğer bir deyişle hangi süreçlerin/konuların önemli olduğunu belirlemek.
II. Risklerin belirlenmesi: Ele alınan süreçteki risklerin ayrıştırmak.
III. Risklerin analizi: Riskleri belli metotlara göre analiz etme ve eğer destekleyici kontroller varsa belirlemek.
IV. Riskleri hesaplama: Artan riskleri belirlemek.
V. Riskleri ele alma: Şirketler tarafından seçilen risklerin azaltılması için riskler ele alınırken izlenen metodu tarif etmektir.

3.1.3. FERMA Risk Yönetimi Standardı ve ISO 31000

Avrupa Risk Yönetimi Dernekleri Federasyonu (FERMA) aralarında Türkiye Kurumsal Risk Yönetimi Derneği'nin de bulunduğu Avrupa'daki ülkelerin önde gelen risk yönetimi derneklerinin kurduğu önemli bir federasyondur. FERMA Risk Yönetimi Standardı, İngiltere'deki Risk Yönetim Enstitüsü (IRM), Sigorta ve Risk Yöneticileri Derneği (AIRMIC) ve Kamu Sektörü Risk Yönetimi Ulusal Forumu (ALARM) kurumlarının temsilcilerinden oluşan ekibin çalışmalarının bir sonucudur. (Topçu, 2010). ISO 31000 ve ISO 73 rehberine göre geliştirilmiştir. ISO 2009 yılında ISO 31000'i yayınlarken aynı zamanda Risk Yönetimi Kullanım Rehberi'ni (ISO/IEC Guide 73) de yayınlamıştır.

FERMA Risk Yönetimi Standardı da AS/NZS 4360 risk standardı gibi beş ana unsurdan oluşur; 1) Risklerin ISO Kılavuzu'na göre değerlendirilmesi, 2) Risklerin belirlenmesi, tanımlanması tahmin edilmesi ve risk profilinin çıkarılması aşamalarını içeren risklerin analizi, 3) Risk yönetim aksiyonlarının belirlenmesi, 4) Risklerin raporlanması ve iletişim prosedürlerinin belirlenmesi, 5) Risk yönetim sürecinin izlenmesi ve gözden geçirilmesi. Kapsamlı bir risk belirleme, tanımlama, değerlendirme ve gerekli aksiyonların belirlenmesi süreci için iyi tasarlanmış bir yapı gereklidir. Risklerin değerlendirilmesi riskin çıkma sıklığı (olasılığı) ve oluşturacağı topyekün etkisi göz önünde bulundurarak yapılmalı ve riskler olasılık ve etkiye göre önemliden daha az önemliye doğru önceliklendirilerek gerekli aksiyonlar belirlenmeli ve hangi durumda hangi aksiyonun alınacağı ve/veya alındığı raporlandırılmalıdır. Raporlama

ve örgüt içi iletişim risk yönetim sisteminin izlenmesi ve gözden geçirilebilmesi için çok önemlidir.



Şekil 7. ISO 31000'e göre Risk Yönetim Süreci

Kaynak: IRM, *Kurumsal Risk Yönetimine (KRY) Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri,* AIRMIC, ALARM, IRM, 2010.

3.1.4. Basel III

Ülkelerin Merkez Bankalarının bir araya gelerek oluşturdukları bir kuruluş olan BIS "Bank for International Settlements" 1974 yılında, bankaların asgari sermaye gereksinimlerini ölçümlemesi için Basel komitesini oluşturmuştur. Basel Komitesi 1988 Yılında Basel I standartlarını yayınlamıştır. 1996 piyasa riski eklemeleri olmuştur, 1998 de ise piyasa riski hesaplaması yürürlüğe girmiştir. Mali piyasaların ve finansal ürünlerin çeşitlenerek gelişmesi sonucu Basel I standartları yetersiz kalmış ve 2004 yılında Basel II standartları oluşturulmuş, Kasım 2005'de revize edilmiştir. Basel II birbirini destekleyen: 1) Asgari sermaye yükümlülüğü, 2) Sermaye yeterliliğinin denetimi ve 3) Piyasa disiplini olarak üç yapısal bloktan oluşmuştur. Basel II ile gündeme gelen ve bankalar tarafından hesaplanması zorunlu olan ve sermaye yeterliliği oranını doğrudan etkileyen kredi riski ölçüm yöntemi olarak iki ana yöntem belirlenmiştir. Göreceli olarak daha kolay olan standart yöntem Avrupa Birliği Üyesi ülkelerde Ocak 2007'de, daha karmaşık olan ileri yöntem ise Ocak 2008'de yürürlüğe girmiştir. Türkiye'de ise bankalar Basel II Standard yöntem ile Sermaye Yeterliliği

Raporu (SYR) hazırlamasına solo olarak Temmuz 2011, konsolide olarak Temmuz 2012'de resmi olarak başlamışlardır. Basel II kriterleri her ne kadar bankaları ilgilendirse de bankalar üzerinde krediye ulaşma açısından şirketler kesimini de ilgilendirmektedir. Kredi riski değerlendirmede artan niteleyici kriterler doğrultusunda ölçme yöntemlerinin de zorluk derecesi standart yöntemden gelişmiş içsel derecelendirme yöntemine doğru artmıştır. Bankaların uygulamak zorunda oldukları yöntemlere göre şirketlerin riskleri daha detaylı değerlendirileceği için şirketler kısmının da risk yönetimine önem vermesi krediye ulaşımı kolaylaştıracaktır.

Tablo 6. Basel II Kredi Riski Ölçüm Yöntemleri

Kaynak: RİSK YÖNETİCİLERİ DERNEĞİ, *Basel II ve Basel II Nedir?*, Basel II ve Türk Eximbank Semineri, 2013.

2008 yılında yaşanan uluslararası finansal krizin hala devam etmekte olan etkileri sonucu yaşanmakta olan likidite sıkıntıları ve akıl almaz kaldıraç oranlarına karşın mevcut düzenlemelerin yetersiz kaldığı görüşü Eylül 2010'da Basel III'ün doğmasına neden olmuştur. 2013-2019 yılları arasında kademeli olarak hayata geçirilecek olan Basel III kriterleri, küresel bir krizin çıkmasına ve yayılmasına engel olamayan Basel II'deki eksiklerin giderilmesini, krize neden olan likidite sıkıntıları ve yüksek kaldıraç oranlarının önüne geçilmeyi amaçlayan ek bir düzenlemedir. Belirlenen ilave oranlar bankaları olağanüstü durumlarda da taahhütlerini yerine getirebilmeleri için gerekli olan güçlü sermaye ve likiditeye sahip olmalarına zorlayan yeni hükümlerdir. Basel III'ün başarısı ise mevzuatı uygulaması beklenen ülkelerdeki yerel otoriteler tarafından gerçekleştirilecek olan denetimler ve yakın takiplere de önemli oranda bağlıdır.

Tablo 7. Basel II ve Basel II Karşılaştırması

Basel II	Basel III
- Basel II – risk ağırlıklı aktiflerin hesabı üzerine şekillendi. Gereksinimler: - Veri biriktirilmesi - Modelleme - Sistem uygulaması	- Basel II'ye ek olarak geliyor - Bankalara etkisi oldukça kapsamlı ve önemli - Sermaye tanımı değişiyor. - Asgari sermaye rasyosu değişiyor. - Karşı taraf kredi riski yaklaşımı değişiyor. - İki adet likidite rasyosu ve 'kaldıraç' rasyosu ileve ediliyor.

Kaynak: RİSK YÖNETİCİLERİ DERNEĞİ, *Basel II ve Basel II Nedir?*, Basel II ve Türk Eximbank Semineri, 2013.

3.1.5. COSO

COSO Amerika'daki muhasebeci ve denetçi birliklerini temsil etmek üzere ve üye kuruluşlara iç kontrol ve hile gibi konular üzerinde üye kuruluşlara rehberlik yapmak amacıyla 1985 yılında kuruldu. Sox-Sarbanes-Oxley kanununun da çıkmasına neden olan Enron ve Worldcom skandallarında görülen hileli finansal raporlama ile kontrol mekanizmasının gittikçe kötüleşmesi üzerine, hileli finansal raporlamanın önlenmesi, iç kontrol, risk yönetimi, kurumsal yönetim ve suiistimali önleme alanlarında kapsamlı bir rehber olan "Enterprise Risk Management–Integrated Framework" (COSO ERM) dokümanını 2004 yayınladı.

2004 yılından bu yana ilk çerçeve rehber yaygın olarak dünya ülkelerinde ve kurumlarda uygulanmış, hedeflenen amaç ve alınan risk tutumu doğrultusunda riskin tanımlanması ve değerlendirilmesi açısından başarılı olmuştur. Ancak riskin strateji ve amaçlarla bütünleştirilmesi yani organizasyon kültürüyle birleştirilerek geliştirilmesi açısından geliştirilmesi gerekliliği söz konusuydu. Özellikle son yıllarda teknolojinin büyük bir hızla gelişmesi, internetin ve mobil iletişimin hayatımızın ayrılmaz bir parçası haline gelmesiyle bilginin çok hızlı bir şekilde yayılması ve bunun sonucu birbirine giren pazarlarla birlikte rekabetin küresel boyutta hızlanması, iş hayatının ve kurumsal yapının karmaşıklaşmasına dolayısıyla iç kontrol ve risk yönetimin değişiklik göstermesine neden olmuştur. 2008'de ABD'de ipotek karşılığı krediler (mortgage) krizi olarak başlayan finansal krizin küresel etkilerini, müşteri taleplerindeki değişimler, çevresel duyarlılığın artması, dijital dönüşüm gereklilikleri gibi pek çok faktör sonucu,

COSO kurumsal yönetim rehberi 2013 yılında revize edilmiştir. 2017 yılında ise çevresel, sosyal ve yönetişimsel (enviromental, social and governance) risklerinde kurumsal risk yönetimiyle bütünleşmesi gerekliliği üzerine tekrar revize edilerek, "Kurumsal Risk Yönetimi- Strateji ve Performansla Entegre Edilmiş" (Enterprise Risk Management—Integrating with Strategy and Performance) adıyla yeniden yayınlanmıştır. 2017 yılında yayımlanan yeni sürümde, değişen çevresel koşulların sonucu ortaya çıkan yeni riskleri kapsayan, karmaşıklaşan risklerin değerlendirilmesini daha açık bir şekilde yapan, paydaşların risk yönetimi farkındalığını artıran bir çerçeve ve daha iyi risk raporlaması getirilmiştir.

COSO Kurumsal Risk Yönetimi Çerçevesi, birbiriyle ilişkili sekiz unsurdan oluşur:

I. Kurumsal Çevre: Kurumun risk kültürü ve risk eğilimine (yönetim tarafından kabul edilebilir riskler) göre kurum içi risk yönetiminin çerçevesini belirler. Kurumun etik değerleri, risk alma kapasitesi, yönetimin çalışma biçimi, görevlerin ve sorumlulukların dağılımı gibi birçok ana girdi faktöründen oluşur.

II. Hedef Belirleme: Kurumsal risk yönetiminin uygulana bilmesi için raporlama, operasyonel ve uyumluluk hedeflerini de içine alacak şekilde gerçekçi amaçların konulması gerekmektedir. Şirketin risk eğilimine göre risk toleransları belirlenir.

III. Gerçekleşmesi Muhtemel Olayları Belirleme ve Tanımlama: Yönetim, strateji, amaç ve performans hedeflerine etki edebilecek olası durumların neler olabileceğini belirler, riskleri ve avantajları ayırır.

IV. Risk Değerlendirme: Negatif etkisi olan riskler ile pozitif etkisi olan fırsatların belirlenmesinden sonra olası etkileri ve ortaya çıkma sıklıklarına göre yani "etki ve olasılık" olarak iki parametreye göre değerlendirilir.

V. Risk Tepkisi: Değerlendirilmesi yapılan risklere verilebilecek cevapları yarar ve maliyet analizine ve eldeki imkanlara göre belirler ve değerlendirir. Etki-Olasılık ölçütüne göre risklere karşı dört adet tepki verilebilir: Riskten Kaçınma, Riski Azaltma, Riski Paylaşma (transfer etme), Riski Kabul Etme.

VI. Kontrol Faaliyetleri: Kurumun bütün fonksiyonlarında ve örgütün bütün seviyelerinde mevcut teknolojik kontrolün genel bilgisi ve uygulamasını içerir. Bir başka değişle risklere verilen cevapların hayata geçirilmesine ve kontrol edilmesine

yardımcı olan risk yönetimi politika ve prosedür faaliyetleridir ve daha çok teknolojik bir yazılım gerektirir.

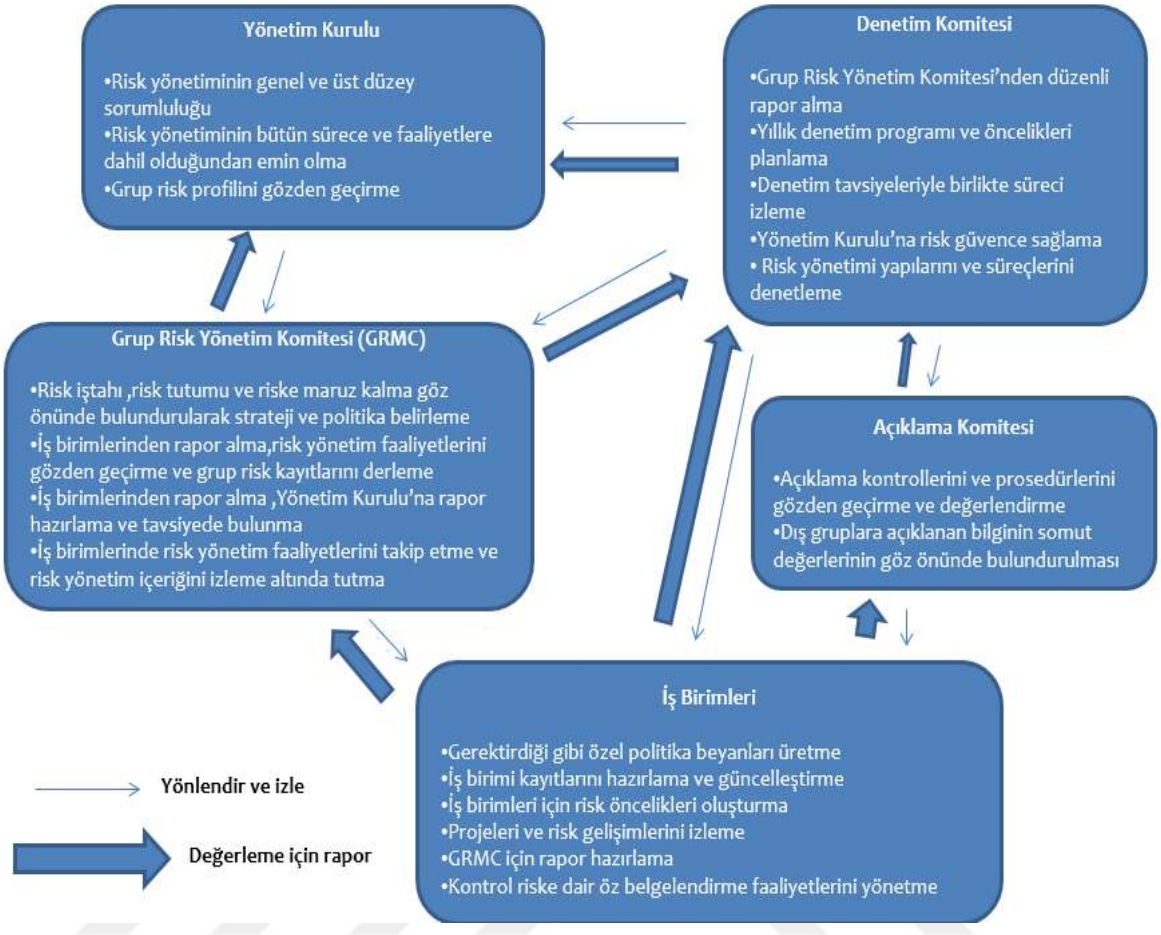
VII. Bilgi ve İletişim: Kurum içi etkin ve zamanında raporlama ve raporların gerekli paydaşlara iletilmesini içerir. Kurum içinde yatay ve dikey bilgi akışının tam ve gerçek zamanda yapılması çok önemlidir.

VIII. Takip: Kurumsal risk yönetim performansının takibi, geliştirilmesi ve iyileştirilmesi için izleme, sürekli izleme faaliyetleri, bağımsız izleme faaliyetleri veya her ikisinin bir birlikteliği şeklinde ortaya çıkar.

COSO kurumsal risk yönetimi çerçevesi basitleştirilerek COSO küpü olarak ta gösterilmektedir. Küpün yatay ekseninde dört hedef kategorisi belirlenmektedir; strateji, operasyonlar, raporlama ve uyum. Dikey eksende süreci oluşturan sekiz aşama bileşeni gösterilir. Kurum seviyeleri, beraber çalışılan tedarikçileri de kapsayacak şekilde kutunun üçüncü boyutunda gösterilmektedir. 2017 yılında yayınlanan yeni çerçevede yönetişim, örgüt kültürü ve bilgi teknolojileri eklenmiş, hedef oluşturmada kurum stratejisi önem kazanmıştır.

3.2.Kurumsal Risk Yönetimi Metodolojisi

Kurumsal Risk Yönetimi metodolojisi, daha önce bahsedilen risk yönetimi standartlarının şirket özeline göre düzenlenip uygulanabilir hale getirilmesi anlamına gelmektedir. Risk yönetimi bir dönüşüm sürecini olup, risklerin birbirimden bağımsız bölümler şeklinde ele alındığı geleneksel bir risk yönetim yaklaşımından, bu risklerin bir bütün olarak şirket stratejisine uygun bir şekilde yönetildiği entegre risk yönetimine geçiş sürecini ifade eder (TÜSİAD, 2008). Bu dönüşüm sürecinin şirket içeresinde başarılı uygulanabilmesi, uygulanacak risk yönetimi metodolojisinin şirket misyonu, stratejileri ve hedefleri ile çevresel faktörlere iyi adapte edilebilmesine bağlıdır. Risk yönetim düşüncesi, davranışı, süreci ve uygulamalarının günlük şirket rutininin bir parçası olması, şirket içi kültürün evrensel kabul gören için risk yönetimi kültürüne adapte olduğunun bir göstergesini oluşturur (Kimbrough, Componation, 2009).



Şekil 8. Şirketler İçin Örnek Risk Yönetim Mimarisi

Kaynak: IRM, Kurumsal Risk Yönetimine (KRY) Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri, AIRMIC, ALARM, IRM, 2010.

Risk Yönetimi Kültürü

Kurumsal Risk Yönetiminden farklı olarak, şirket kültürü işletme yönetimi teoreminin bir parçasıdır ve şirket tarafından ortaya çıkarılan değer, sorumluluk pozisyonunda olanların liderlik biçimleri veya şirket içi kullanılan yönetim dili olarak açıklanmaktadır. Şirket kültürü üzerine yapılan araştırmalar şirket kültürünü yönetimin çalışanlara karşı tavrını ya da bölümler arasındaki davranış biçimine odaklanmaktadır. Hangi bakış açısından bakılırsa bakılsın, çalışanların hangi durumda öncelikleri belirleyip nasıl uygulamaya aldıklarını şirket kültürü belirler. Örneğin, pazardaki değişimlere şirket tarafından ne kadar hızlı cevap verildiği, ne kadar başarılı veya başarısız iş çevrelerindeki değişime uyum sağlayıp yol kat edildiği şirket kültürünün bir parçasıdır (Kimbrough, Componation, 2009).

Kurumsal risk yönetimi ise belirsizlik dönemlerinde şirket yönetimlerine gerekli esnekliği sağlayarak şirketlerin dayanıklılıklarını artırdığı için şirket kültürünü birebir etkileyerek, risk yönetimi kültürü haline dönüştürmektedir. Miccolis 2003 yılında sunduğu çalışmasında risk yönetimi üzerine yaptığı ankete cevap verenlerin yarısının kurumsal risk yönetimi uygulaması önündeki en önemli engelin şirket kültürü –başka bir değişle şirket içinde kemikleşmiş davranış biçimleri- olduğunu belirttiklerini söylemiştir (Miccolis, 2003). Kurumsal risk yönetimin karar alma sürecinin alt biriminden en üst yetkilisine kadar kapsayıp onların çalışma şekillerini değiştirdiği düşünülürse, şirket kültürü üzerinde köklü bir değişikliği getirmesi kaçınılmazdır. Uygulamada en zor değişimlerin alışılmış davranışların değiştirilerek yeniliklerin günlük rutin içinde kabul edilmesi olduğu düşünülürse, risk yönetimi uygulamasında en önemli bariyerin mevcut şirket kültürü olması kaçınılmazdır.

Tablo 8. Risk Kültürü Oluşumu Aşamaları

Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004

Risk yönetimi kültürünün geliştirilmesi şirket içi risklere karşı farkındalık, yetkinlik, yeterlilik, beceri ve bilginin geliştirilmesini içermektedir Başarılı bir risk kültürü uygun bir risk mimarisi, stratejileri, taktiksel ve operasyonel hedefleri, risk yönetim sorumlulukları, protokolleri kurularak kazanılır (IRM, 2010). Bu kültür hesap verilebilirliği, performans ölçümünü, ödülü ve her seviyede operasyonel verimliliğin ilerlemesini desteklemelidir. Bu kültürü aşılayabilmek için uygulanan yöntemler aşağıdaki şemada gösterilen dört ana başlıkta gruplanabilir.

3.2.1. Risk İştahı

Yatırımcıların risk taşıma istekliliği olarak tanımlanabilen risk eğilimi, şirket düzeyinde şirketin risk kapasitesi göz önünde bulundurularak kendi misyonları doğrultusunda, hedef ve stratejilerini gerçekleştirmek için karşılaşılan her bir risk türü itibarıyla taşınmak istenen risk düzeyini ifade eder. Başka bir değişle, şirketin paydaşlarının, yönetiminin ve bir bütün olarak çalışanların riske karşı tutumunu yansıtır.

Şirket içinde bulunduğu sektöre, genel ekonomik duruma, büyüme hedefleri ve maruz kalınacak riskin getirisi bakımından analizini yapıp, yönetim kurulunun belirlediği hedefler doğrultusunda yüksek, orta, düşük şekilde risk eğilimini belirler. Risk ile getirinin doğru orantıda olması şirketlerin risk eğilimini artırırken, belirsizlikten kaynaklanan olası kayıpların göz ardı edilmemesi gerekmektedir. Risk isteği, kaynakların bölümlendirilmesine de neden olur. Yönetim risk eğilimini –almak istediği risk limitini- kurumun finansal kapasitesine, beklenmedik olaylar karşısında ne kadar dayanıklı olduğuna, ileri dönemli büyüme planlarına ve içinde bulunduğu ekonomik çevreye göre değerlendirmeli, etkili bir şekilde riskleri ele alıp ona karşılık verebilmek için altyapı oluşturmalıdır (PWC, 2006).

Risk eğilimini hissedarların beklentilerine, geçmiş tecrübelere, bölümlerin hayatta kalabilme tehdidine uğramasına, yeni risk alanlarının doğmasına ve yöneticilerin kişisel risk eğilimine bağlıdır (Güneş, 2009). Objektif olmayan bir şekilde kişisel etkilerle gereğinden fazla belirlenmiş risk eğilimi yatırımcıların parası ile kumar oynamaya benzetilebilir. Kurumsal risk yönetimi risk eğilimini kumar oyunundan rasyonel bazlı bir fırsat değerlendirmesine çevirecek bir şekilde yansız ve açık olarak belirler.

3.2.2. Risk Toleransı

Risk toleransı, riskin ortaya çıkması sonucunda yaşanan kaybın şirket kaynaklarınca sorunsuzca karşılanabilmesi için gereken kurumsal ve finansal yeterlilik olarak tanımlanabilir. En basit anlamıyla şirketin almak istediği riski gösteren "risk eğilimine" karşılık, şirketin kurumsal ve finansal olarak risk taşıma kapasitesi (limit) "risk toleransını" belirler. Başka bir deyişle şirketin risk toleransı, organizasyon için kabul edilebilir olan riske karşılık gelir (PWC, 2006).

Risk toleransı performans hedefleri yardımıyla ölçülebilir ve yönetime risk eğilimi limitlerini açık bir şekilde gösterdiği için, hedefleri gerçekleştirmek için kabul edilemeyecek boyutta bir risk alınmaması konusunda çok daha fazla güvence sağlar. Yönetim her aşamada kendilerine uygun risk değerlendirme metotlarına göre riskleri niteliksel ve niceliksel olarak değerlendirerek, riskin ortaya çıkma olasılığına ve ortaya

çıkarsa meydana gelecek zarara, buna karşı şirketin kurumsal ve finansal kapasitesine göre her olası risk için tolerans sınırları belirlenmelidir.

Belirlenen risk tolerans sınırları çerçevesinde şirket risklere karşı nasıl aksiyonlar alacağını tanımlamalı ve prosedürlerle açık bir şekilde kayda almalıdır. Belirlenen aksiyonların her zaman minimum ölçüde risk sonuçlarını ortaya çıkarması gerekmez ama risk toleransı düzeyini aşmaması gereklidir. Risk toleransı ve gerekli aksiyonların belirlenmesi, uygulanması ve raporlanması şirket içi iletişim stratejisinin oluşturulması ile mümkündür. (Güneş, 2009). Etkin bir iletişim stratejisi, iletişimin bütünsel, gerçek zamanlı ve şeffaf bir şekilde gerekli bütün paydaşları içerecek şekilde yapılmalı ve uygulanmalıdır.

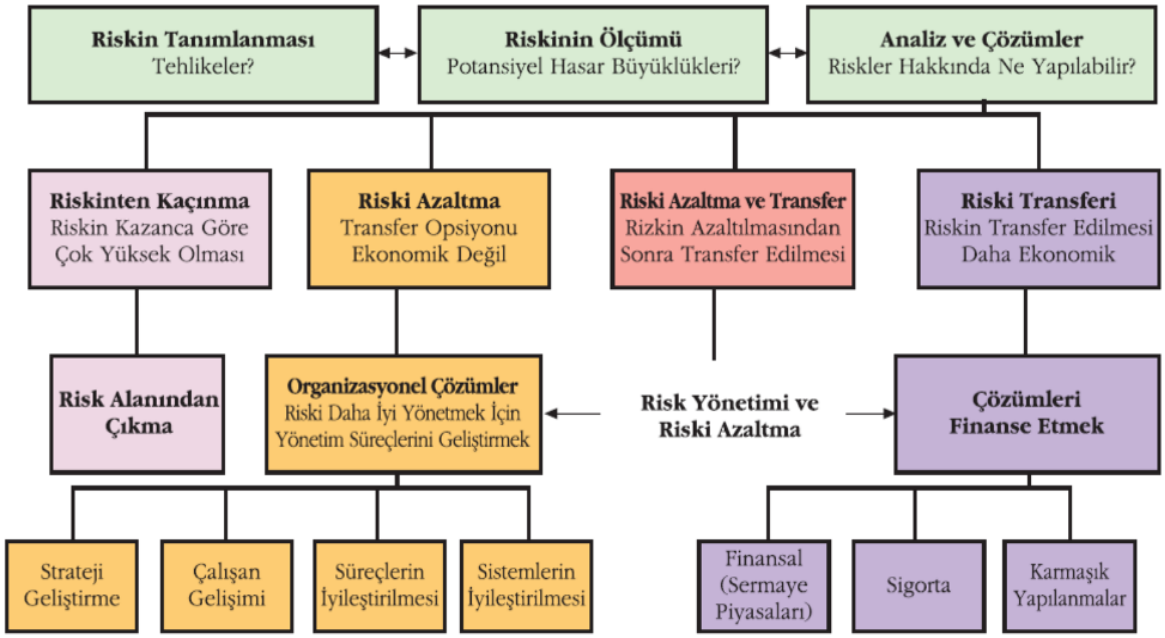
3.2.3. Kurumsal Risk Yönetimi Döngüsü

Kurumsal risk yönetimi sürekli değerlendirme, geri besleme (feedback) ve geliştirme döngüsü içeresinde dinamik bir olgu olarak düşünülmelidir. Bu döngü, misyon ve vizyona bağlı olarak stratejik hedeflerin, ne, ne zaman ve nasıl sorularına yanıt verecek şekilde planlanması ile başlar. Risk belirleme metotlarına göre risklerin tanımlanması, risk değerlendirme metotlarına göre risklerin derecelendirilip gerekli aksiyonların belirlenmesi aşamaları ile devam eder. En son risk denetleme ve raporlama aşamasında risklerin raporları, alınan aksiyonlar ve elde edilen sonuç gözden geçirilerek sürecin iyileştirilmesi ile döngü tamamlanır.

Risk yönetimi süreci İngilizce kaynaklarda kısaca 7R ve 4T[3] ile tanımlanmıştır. Türkçe özetlersek; Risklerin tanımlanması, Risklerin sıralanması, Riske gerekli müdahalelerin (aksiyon) belirlenmesi, Gerekli aksiyon için kaynak ayırılması, Beklenmedik riske karşı reaksiyon alınması, Risk performansının raporlanması ve Risk yönetim çerçevesinin gözden geçirilmesi yedi R'yi oluştururken riske cevap verme (responding) aşaması dört T ile tanımlanan aksiyonlar ile yapılmaktadır. Risk toleransı limitleri içinde olan riskler için aksiyon almayarak kabullenme, tolerans limitleri üzerinde olan ve bertaraf edilebilecek riskler için müdahale ederek etkisini azaltma,

[3] 7R ve 4T risk için kullanılan İngilizce kelimelerin baş harflerinden oluşturulmuştur. Recognition, Ranking, Responding, Resourcing, Reaction, Reporting, Reviewing ve Tolerate, Treat, Transfer, Terminate

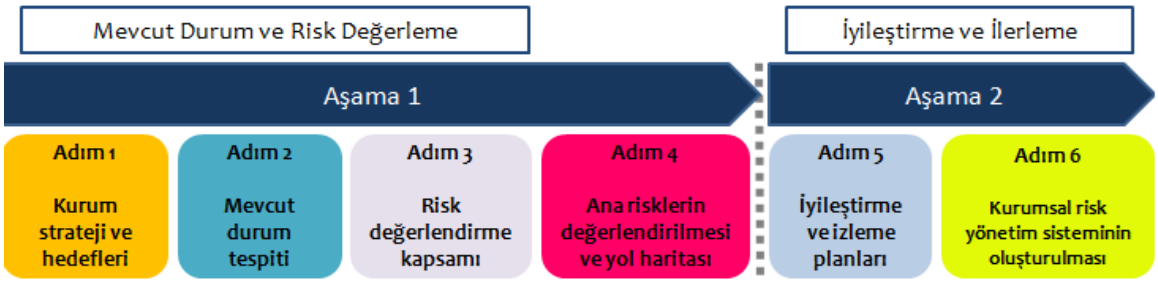
etkisi azaltılamayacak riskleri transfer etme ve yıkıcı etkisi çok yüksek olan riskleri (insan hayatını tehdit eden riskler gibi) sonlandırma.



Şekil 9. Örnek Risk Yönetimi Süreci

Kaynak: TÜSİAD, Kurumsal Risk Yönetimi, Lebib Yalkın Yayımları ve Basım İşleri A.Ş., İstanbul, 2008.

Risk yönetimi sürecinin başarılı ve etkin olabilmesi için öncelikle risk yönetim sürecinin işletmenin misyon ve vizyonu, ileriye dönük hedefleri ve bu hedeflere ulaşma stratejileri, faaliyetlerin karmaşıklık seviyesi, finansal yapısı, işletme kültürü, sektör uygulamalar, yasal düzenlemeler, çevresel faktörler, insan kaynaklarının nitelik ve niceliği, işletmenin içinde bulunduğu durumu ele alarak planlanması gerekmektedir.



Şekil 10. Entegre Risk Yönetimi'nin Uygulanması

Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004

Planlamanın birinci aşaması olarak işletmenin risk yönetimi stratejisi oluşturulmalı, risk yönetiminin hedefleri, işletmenin risk eğilimi ve tolerans limitleri,

risk yönetim sürecinin nasıl organize edileceği, risk yönetim sürecine katılanların görev ve sorumlulukları ve nasıl eğitilecekleri, denetimin ve yaptırımların nasıl olacağı açık bir şekilde belirlenmelidir. Bu aşamada ayrıca risk yönetim araçları ve metodolojileri de belirlenerek risk göstergeleri tanımlanmalıdır (Köksal, 2013). Risk mimarisi, strateji ve protokollerinin detayları kurumun risk yönetim politikasına kayıtlı olmalıdır. Klasik bir risk yönetim politikasının içeriği (IRM, 2010):

- Risk yönetimi ve iç kontrol hedefleri (yönetişim)
- Kurumun riske karşı davranış tarzının beyanı (risk stratejisi)
- Risk farkındalığı kültürünün veya denetim ortamının açıklaması
- Seviye ve mahiyeti kabul edilebilir risk (risk eğilimi)
- Risk yönetimi organizasyonu ve prosedürler (riski mimarisi)
- Riski tanıma ve sıralama işlemleri ayrıntıları (risk değerlendirme)
- Risk analizi ve raporlama için belgeler listesi (riski protokolleri)
- Risk azaltma gereklilikleri ve kontrol mekanizmaları (risk tepkisi)
- Risk yönetimi rollerinin ve sorumluluklarının tahsisi
- Risk yönetimi eğitim konuları ve öncelikleri
- Risklerin izlenme ve karşılaştırma ölçütleri (kıyaslama)
- Risk yönetimi için uygun kaynakların tahsisi
- Risk faaliyetleri ve önümüzdeki yıl için risk öncelikleri

3.2.4. Risk Belirleme Teknikleri

Risk kontrol edilebilmesi için öncelikle açık bir şekilde tanımlanması, etkisinin ve ortaya çıkma olasılığının belirlenmesi gerekmektedir. Genellikle, yönetim ekibi, şirkete genel olarak baktıkları için süreç bazlı spesifik riskleri kestirebilme kabiliyetinden yoksun olabilir. Şirket yönetiminin başarılı olabilmesi için birincil şart olası riskleri kontrol edebilmek için risklerin ne olduğu net olarak tanımlanması gerekir (Topçu, 2010). Risk tanımlama teknikleri hem mevcut durumu, hem geçmişi hem de geleceği dikkate almaktadır. Geçmişe dayalı risk tanımlama teknikleri geçmişteki hasarlar ve mali kayıpları değerlendirebilirken geleceğe yönelik teknikler ise yeni piyasa koşulları ve rakip aksiyonları gibi bilgileri ele alabilir. Mevcut durum ve geçmişe yönelik tanımlamalar raporlama sisteminin bir parçası iken, gelecekle ilgili değerlendirmeler stratejik planlamanın bir parçasıdır.

Tablo 9. Risk Belirleme Teknikleri

Teknik	Açıklama
➢ Anketler ve kontrol listeleri	• Yapılan anketlerin ve kontrol listelerinin belirgin risklerinin tanımlanmasını desteklemek üzere bilgi toplamada kullanımı
➢ Atölye çalışmaları ve beyin fırtınası	• Fikirlerin toplanması ve paylaşılması; hedefleri, paydaş beklentilerini veya kilit bağımlılıkları etkileyebilecek olayların tartışılması
➢ Teftişler ve denetimler	• Önceliklerin ve aktivitelerin fiziksel teftişleri, yapısal sistemler ve prosedürlerle uygunluğun denetimi
➢ Akış şemaları ve bağımlılık analizleri	• Başarının anahtarı olabilecek kritik bileşenlerin tanımlanması amaçlı organizasyon içi süreçlerin ve faaliyetlerin analizi
➢ HAZOP ve FMEA görüşleri	• Tehlike ve İşletilebilirlik çalışmaları ve Arıza Modu Etkileri Analiz nicel teknik arıza analiz teknikleri
➢ SWOT ve PESTLE analizler	• Güçlü yanlar Zayıflıklar Fırsatlar Tehditler(SWOT) ve Politik Ekonomik Sosyal Teknolojik Yasal Çevresel (PESTLE)analizleri risk tanınmasına yapısal görüşler sunar

Kaynak: IRM, *Kurumsal Risk Yönetimine (KRY) Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri,* AIRMIC, ALARM, IRM, 2010.

Tablo 9'da görüldüğü gibi risklerin belirlenmesinde değişik bilgi toplama ve değerlendirme teknikleri kullanılmaktadır. Şirket tarafından uygulana bilirlikleri ve işe yarar sonuçlar elde edilmesi teknik seçiminde önemli noktalardır. Risklerinin belirlenmesinde en etkin yol, süreç odaklı bir yaklaşım izlemektir. Dolayısıyla kurum süreçlerinin detaylı bir şekilde belirlenmesi ve her süreçteki mevcut durumun tarafsız bir şekilde tanımlanması gerekmektedir. Bundan sonra sürecin amacının, varlık nedeninin belirlenmesi, süreç akış şemasının çıkarılması, sürecin müşterilerinin belirlenmesi ve süreç göstergelerinin belirlenmesi gerekmektedir (ÇSGB, 2013).

Sadece riskler değil bu süreçte başarıda kilit rol oynayabilecek faktörlerin, hedeflere ulaşmadaki tehditlerin ve fırsatların da belirlenmesi gerekmektedir. Kurumda katma değer yaratabilecek bütün aktiviteler tehdit ve fırsatlar olarak değerlendirilerek, oluşabilecek bütün riskler tanımlanmalıdır (IRM, 2010). Riskleri tanımlama yöntemlerinden anket uygulaması geçmiş tecrübelerin ve uygulamaların verilerini elde etmek için sıklıkla kullanılan ve COSO uygulamasının önemli bir parçası olurken,

SWOT ve PESTLE stratejik planlanmanın bir parçası olarak, geleceğe yönelik risk ve fırsatların tanımlanmasında yaygın bir şekilde kabul görmektedir. Diğer bir yöntem olan teftiş ve denetim raporları daha eski anlayış olan statik risk yönetiminin bir parçası olarak sıklıkla kullanılmaktadır. Riskli tabir edilen rafineri, tersane gibi kurumlarda HAZOP, üretim yapılan kurumlarda FMEA yöntemi kullanılmaktadır.

Risklerin tanımlanmasında 2012 yılında yürüklüğe giren 6331 sayılı İş Sağlığı ve Güvenliği Yasası ve bağlı yönetmelikler önemli bir kılavuz olarak kullanılmalıdır. 2012 yılında yayınlanan yönetmelikte risklerin değerlendirilmesi için çalışma ortamı, çalışanlar ve işyerine ilişkin ilgisine göre asgari olarak şu bilgilerin toplanması gerektiği vurgulanmıştır: a) İşyeri bina ve eklentileri, b) İşyerinde yürütülen faaliyetler ile iş ve işlemler, c) Üretim süreç ve teknikleri, d) İş ekipmanları, kullanılan maddeler, artık ve atıklarla ilgili işlemler, e) Organizasyon ve hiyerarşik yapı, görev, yetki ve sorumluluklar, f) Çalışanların tecrübe ve düşünceleri, g) İşe başlamadan önce ilgili mevzuat gereği alınacak çalışma izin belgeleri, h) Çalışanların eğitim, yaş, cinsiyet ve benzeri özellikleri ile sağlık gözetimi kayıtları, genç, yaşlı, engelli, gebe veya emziren çalışanlar gibi özel politika gerektiren gruplar ile kadın çalışanların durumu, i) İşyerinin teftiş sonuçları, j) Meslek hastalığı ve iş kazası kayıtları, k) İşyerinde meydana gelen ancak yaralanma veya ölüme neden olmadığı halde işyeri ya da iş ekipmanının zarara uğramasına yol açan olaylara ilişkin kayıtlar, l) Ramak kala olay kayıtları, m) Malzeme güvenlik bilgi formları, n) Ortam ve kişisel maruziyet düzeyi ölçüm sonuçları, o) Varsa daha önce yapılmış risk değerlendirmesi çalışmaları, p) Acil durum planları, q) Sağlık ve güvenlik planı ve patlamadan korunma dokümanı gibi belirli işyerlerinde hazırlanması gereken dokümanlar (Resmi Gazete Sayı 28512, 2012).

3.2.5. Risk Değerlendirilmesi

Risk değerlendirmesi, riskler belirlendikten sonra risk ölçüm metotlarına göre risklerin ortaya çıkma olasılıklarının ve zaman, maliyet, performans ve itibar açısından olası gerçekleşebilecek hasarın ölçülmesi ve ölçüm sonuçlarına göre sınıflandırılması faaliyetlerini içerir (ÇSGB, 2013). Sınıflandırılan riskler 3.2.4. bölümde 4 T[4] olarak

[4] En riskliden daha az riskliye göre alınacak aksiyonlar: Sonlandırma (Terminate), Transfer etme (Transfer), Müdahale etme (Treat), Kabul etme (Tolerate).

belirlenen aksiyonlara bağlı olarak, tanımlanmış risklere karşı alınacak kontrol faaliyetleri belirlenir.

Tablo 10. Şirketlerin Maruz Kaldığı Risklerin Değerlendirme Şablonu

Dışsal Faktörler				
Makro-Ekonomik	Kurum ve Regülasyonlar	Rekabet	Market	Riziko Riskleri
• Ekonomik düşüş •Enflasyon •Mali piyasa	• Piyasa mevzuatı •Vergi, yasal değişiklikler •Politik huzursuzluk •Sosyal bunalımlar	• Rekabet artışı •Tüketici talep değişikliği •Teknolojik yenilik	• Faiz oranı değişkenliği •Döviz •Temettü fiyat riski •Emtia riski •İtibar & karşı taraf	• Doğal afetler •Hava koşulları •Terörizm / Vandalizm •Harici kazalar

Stratejik Riskler	Operasyonel Riskler			
•İş modeli ve stratejik planlama •Yönetim modeli •Şirket birleşmeleri ve satın almaları •İttifak yönetimi •Yatırım değerlendirmeleri •Teknolojik araştırma ve geliştirme •Reputasyon riski •Sınır ötesi işbirliği riski	Süreç Riski			
	•Pazarlama & iletişim •Ürün/servis yönetimi ve geliştirmesi •Şebeke	•Şebeke güvenliği & güvenilirliği •İş kesintisi •Tedarik ve lojistik riskleri •Tedarik zinciri riski	•Sözleşme dönemi & koşulları •Şebeke kapasitesi •Hareket işleme	•Çevresel risk •Bilgi yönetimi •Müşteri memnuniyeti •Faturalandırma & Tahsilat
Finansal Riskler	İnsan Kaynakları Riski	Kanuni Uygunluk	Bilgi Sistemi Riskleri	Raporlama Riskleri
•Borç / öz sermaye rasyosu •Yeterlilik riski •Likidite / nakit akış riski •Taahhütname / teminatlar •Finansal skorun düşme riski	•Yetkinlik ve beceriler •Yükümlülük •Tazminat / teşvik •Çalışanların verimli kullanılamaması •Başarı planlaması •İşe alım / alı koyma •Eğitim	•Şirket politika ve prosedürlerini ihlal edilmesi •Yönetim / çalışan / 3. şahıs dolandırıcılıkları •Gayri meşru hareketler •3. şahıs hırsızlıkları •Regülasyonlarla uygunsuzluk •Yasal takibat	•Bilgi sistemi veri güvenliği •Bilgi sistemi ulaşılabilirliği / kullanılabilirliği •Bilgi sistemi yönetimi / inovasyon •Elektronik bilgi değişim verimliliği ve güvenilirliği	• Yatırımcı ilişkileri •Denetimsel raporlama •Bütçe / gelecek tahmini •İş performansının izlenmesi

Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004

Riskleri değerlendirirken ayrıca endüstrideki en iyi örnek uygulamaların (benchmark) ve sektörel envanterin kullanılması daha spesifik bir bakış açısı getireceği için risklerin sınıflandırılmasını kolaylaştıracaktır. Bu durum, sektöre özel gözden kaçırılabilecek risklerin de gündeme getirilmesi anlamında faydalı olacaktır. Diğer yandan endüstriyel olarak sektörel bazlı toplanan bilgi finans, satın alma, pazarlama gibi fonksiyonel riskleri de kapsamalıdır.

Risklerin değerlendirilmesi ve sınıflandırılmasın da göz önüne alınması gereken üç ana neden vardı: a) Şirketin amaçlarının yaratacağı etkileri tayin etmek ve hesaplamak; b) Risk toleransını saptamak; c) Son olarak da riskleri önceliklendirmektir. Risklerin önceliklendirilmesinin amacı, risklere karşı hangi aksiyonların alınacağını, hangi riskin öncelikli olarak iyileştirilmesi gerektiği konularında karar vermek için gereklidir. Riskin derecelendirilmesinde ilk iş şirketin karşılaşabileceği olası kayıpları

bulup, bu kayıpların ortaya çıkma olasılıkları ve şiddetini değerlendirmektir (Topçu, 2010).

Risklerin ölçülmesi için kullanılacak analiz yöntemi, analiz edilecek riske, analizin amacına, sahip olunan mali kaynaklar ve bilgi birikimine bağlı olarak farlılık göstermektedir. Analizin durumuna göre niteleyici, yarı-niceleyici, niceleyici veya bunların bütünleşimi olan karma yöntem olabilir. Bu analiz tiplerini karmaşıklık (yüksek bilgi birikimi isteyen yöntemler karmaşık olarak nitelendirilmektedir) ve maliyet özelliklerine göre, en zor ve maliyetliden en az ve düşük maliyetliye doğru sıralarsak: yüksek bilgi birikimi ve teknolojik alt yapı isteyen kantitatif yöntemler, daha az maliyetli ve karmaşık olan yarı kantitatif yöntemler ve nispetten uygulaması daha kolay olan ama mutlak (matematiksel) sonuçlar veremeyen kalitatif yöntemler.

Uygulamada niteleyici çözümleme genelde riskin derecesi hakkında bir ön tahmin edinilmesinde ve önemli risk alanlarının tespit edilmesin de kullanılır. Bununla birlikte itibar riski gibi soyut risklerde kalitatif yöntemler kullanılmaktadır. Önemli arz eden ve somut içerikli ve özellikle finansal risk alanlarında daha spesifik veya kantitatif analizler kullanılmaktadır. Eğer ortaya çıkması muhtemel olmasına rağmen elde bulunan bilgiler yetersiz ve güvenilir değil ise, riskin çıkma sürecine dahil bireylerin veya grupların tahminlerine dayandırılan analizler yapılabilir. Bu tip analizlerde ilgili paydaşların tahminleri arasında bir denge sağlanması gereklidir (TÜSİAD, 2008).

3.2.6. Riskleri Ölçme Metotları

Riskleri ölçme metotları, başka bir deyişle risklerin değerlendirilmesi risklerin ortaya çıkma olasılığı, gerçekleşmesi durumunda olabilecek etkilerinin tahmin edilmesi ve yönetimini kapsayan bir aşamadır. Bu sürecin sonunda risk matrisi[5] çıkarmak için gerekli bilgiye ulaşılır. Bu aşamada risklerin, zaman içinde gerçekleşme olasılığı

[5] Risk matrisi ilk önce ABD'de Askeri standardının sistem güvenlik ihtiyaçlarının karşılanması amacıyla geliştirilmiş olup, mevcut tehditlerin gerçekleşme olasılıkları, meydana gelmesi halinde ortaya çıkacak zararın tespit edilmesi ve tehditlerin kabul edilebilir olup olmadıklarının ortaya çıkarılması amacıyla kullanılan toplulaştırılmış bir tablodur.

(ortaya çıkma sıklığı) ve şirkete yapacağı etki (finansal olarak ölçülmeye çalışılır) risk ölçme metotları yardımıyla tespit edilmekte ve sınıflandırılmaktadır (Köksal, 2013).

Bir önceki bölümde bahsedildiği gibi uygulaması ve maliyeti az olan kalitatif yöntemlerin yanında uygulaması daha zor (teknik bilgi ve alt yapı gerektirdiği için) ama net ve matematiksel bir şekilde ölçüm yapılmasını sağlayan kantitatif yöntemler aracılığıyla risklerin etkileri ölçülmektedir. Hatta finansal veya finans dışı tüm şirketlerin risk yönetimine ilişkin senaryo analizi ve stres testi gibi daha ileri analitik metotları da kullanmaları gerekmektedir. Bu metotlar sayesinde risklerin ne büyüklükte olduğu ve şirketin karlılığı üzerindeki etkileri sayısallaştırıla bilmektedir. Sayısal bir şekilde somut hale getirilen riske karşı şirket, riski üstlenip üstlenmeyeceğine, riskten kaçınıp kaçınmayacağına veya riski belirli bir seviyede tutup tutmayacağına daha rasyonel bir şekilde karar verebilecektir.

Üstlenilen riskler sonucu ortaya çıkan kayıplar için mevcut bulunan işletme sermayesine risk sermayesi denilmektedir. Riskleri üstlenmek için gerekli olan risk sermayesinin belirlenmesi için şirket risk toleransına göre senaryo analizleri yapılır ve daha çok en kötü senaryolar dikkate alınarak risk sermayesi ayırılır. Risk sermayesinin finansal bir yükümlülük yani maliyet getirdiği göz önüne alındığında, gereğinden fazla karamsar varsayımlarla yapılan senaryonun gereksiz maliyet yükü getirdiği, gereğinden fazla iyimser yapılan senaryoların ise sermaye eksikliğinden dolayı daha bertaraf edilemeyen riske bağlı olarak daha fazla maliyet getirdiği görülmektedir. Dolayısıyla senaryo analizlerinin gerçekçi varsayımlarla ve gerekli teknik altyapı kullanılarak (gelişmiş istatistik programları gibi) yapılması çok önemlidir. Başka bir deyişle, senaryo analizlerinde dikkat edilmesi gereken nokta, gereğinden yüksek risk sermayesi, karlılığın azalmasına yol açarken, risk sermayesi açığı da şirketin yükümlülüklerini yerine getirememe riskini artırır (Topçu, 2010).

3.2.6.1. Etkiler ve İhtimal

Bir olay birden çok sonuç doğurabileceği gibi farklı iş hedeflerini etkileyen sonuçlara yol açabilir. Etki ve olasılığın tahmin edilebilmesinde istatistiksel analiz ve hesaplamalar kullanılabilir (Güneş, 2009). Analiz anında belirlenmesi gereken en önemli bulgulardan biri olayın ortaya çıkma ihtimalidir.

$$Olasılık\ (\pi) = \frac{Olayın\ \ tekrarlanma\ sayısı\ (n)}{Aynı\ zamandaki\ toplam\ işlem\ sayısı\ (N)}$$

Buradaki en büyük varsayım geleceğin geçmişin kopyası olduğunu düşünmektir. Başka bir değişle belirli bir olayın gelecekte ortaya çıkma olasılığının geçmişteki gibi olacağı varsayılmaktadır. Ancak değişen ürün ve hizmetler ile piyasa durumları ve teknolojide meydana gelmekte olan farklılıklar düşünüldüğünde, bu varsayımın her zaman geçerli olmadığı rahatlıkla görülebilir. Bu yöntem sadece sürekli meydana gelen olayların tahmin edilebilmesi için daha geçerli olabilir. Diğer olaylar için senaryo analizi yapmak daha geçerli bir yöntemdir.

3.2.7.2. Senaryo Analizi

Gelecek senaryoları, geleceği tam bir bilinmezlikten kurtarmak ve hesaplanabilir gelecekler kurmak için gerçekçi varsayımlar üzerine geliştirilen kurgulardır (Aşçı, 2017). Beklenmedik bir olay olarak tabir edilen risklerle ilgili genellikle üç çeşit kurgu geliştirilir. Ortaya konulan kurgular aynı zamanda senaryo olarak da adlandırılır. Belirli varsayımlar üzerine ilerletilen her senaryo için beklenmedik olayların ortaya gelme ihtimali ve etki değerleri hesaplanmaya çalışılır. Gelecek senaryosu geçmiş ile ilgili bildiklerimizin geleceğe taşınması değildir. Geçmiş bize gerçekçi modeller oluşturmamız için veri sağlayarak, gelecek ile ilgili senaryo yaratma için gerekli alt yapıyı oluşturur.

Daha çok sübjektif nitelik taşıyan bu hesaplamalar doğrultusunda operasyonel risklerin olası büyüklükleri belirlenmeye çalışılmaktadır. Senaryo analizlerinde kullanılan varsayımların gerçeği yansıtabilmesi ancak önemli bir bilgi birikimi ve teknolojik alt yapı ile sağlanabilir.

3.2.7.3. Riske Maruz Değer (RMD)

Kantitatif yöntemler arasında yer alan ve finansal riskleri hesaplamak için riske maruz değer tamamıyla istatistiki bir yöntemdir. Normal piyasa koşullarında, belirli bir zaman aralığında ve belirli bir güven düzeyinde[6] ortaya çıkması beklenen en kötü finansal kayıp tutarını hesaplamak için kullanılır. Daha çok bankalar, sigorta şirketleri

[6] Bu yöntemde kullanılan istatistiki olasılık dağılımı normal dağılım olarak anılan "Standart Gaussian Dağılımıdır" ve güven aralığı % 95 veya % 99 olarak belirlenir. Başka bir değişle hesaplamada hata yapma olasılığı olarak ta adlandırılan α % 5 veya % 1 olarak sabitlenir.

ve aracı şirketler tarafından kullanılan bu yöntem, gerekli alt yapısı olan şirketler tarafından özellikle finansal kararların doğuracağı olası kayıpları hesaplamak için kullanılmaktadır.

Bu yöntemde risklere bağlı kayıpların ortaya çıkma olasılığının normal dağlım olarak bilinen simetrik bir yapıda olan standart Gaussian dağılımına uyduyu varsayılmaktadır. Hangi olasılıkta hangi kaybın oluşacağı üç ayrı metotla belirlenmektedir: tarihsel simülasyon (geçmişteki veriler kullanılan gerçekleştirilen simülasyon), Monte-Carlo simülasyonu (istatistiki programlar kullanılarak yapılır) ve analitik yaklaşım (standart normal dağılımdan gelen verilerle yapılır).

3.2.7.4. Duyarlılık Analizi

Hem senaryo analizinde hem de riske maruz değer hesaplamasında kullanılan varsayımlar kesin ve kusursuz olması imkansızdır. Dolayısıyla içinde bulunulan ortamın değişmesi ve farklılaşması sonucu varsayımlar ve kullanılan verilerin nasıl etkileneceğini belirlenmek için duyarlılık çözümlemesi yapılmalıdır. Duyarlılık çözümlemesi aynı anda belirlenen riske karşı oluşturulan aksiyonların ve kontrollerin uygunluğunu ve etkinliğini test etmek için de kullanılabilmektedir.

Basit bir anlatımla duyarlılık analizi belirli piyasa senaryoları altında finansal pozisyonu hesaplamak için kullanılan modelin tepkilerini belirlemek için kullanılır. Bu şekilde piyasadan gelen bir şok dalgalarının şirketin finansallarını nasıl etkileyeceği belirlenmeye çalışılır. Örneğin, Temmuz 2018'de yaşanan TL'nin USD karşısında erimesi şokunun özellikle dış açığı olan bir şirket üzerinde telafi edilmesi güç kayıplara yol açması duyarlılık analizi ile öngörülebilir.

3.2.7.5. Kalitatif Analiz

Kalitatif analiz, istatistiki hesaplamalar yapılması için gerekli sayısal verinin olmadığı, soyut olaylar için ya da şirketteki bilgi birikimi ve teknik alt yapı yeterli düzeyde olmadığı zaman kullanılan yaygın bir yöntemdir. Risk düzeyi detaylı bir çözümleme de kullanılan zaman ve emeği karşılamadığı zamanda maliyet azaltması için kalitatif analiz kullanılmaktadır. Risklerin potansiyel etkilerinin derecesi ve bunların ortaya çıkma ihtimalleri, çoğunlukla beşli skala üzerinden katılımcıların bireysel

yargıları ile değerlendirilmektedir. Bu skalalar ihtiyaca veya risklerin özelliklerine göre değiştirilerek kullanılabilir (TÜSİAD, 2008).

Kalitatif yaklaşımlar anahtar göstergeler, yarar-değer çözümlemesi, karar ağacı çözümlemesi (sübjektif), senaryo çözümlemesi (sübjektif), süreç çözümlemesi ve uzman görüşlerinin toplandığı risk çayıştayından oluşmaktadır.

3.3. Risk Yönetimi Sürecinde Görev Dağılım ve İletişim

Risk yönetimi için oluşturulan yapı, kurumun büyüklüğü, risk kültürü, içinde bulunduğu sektör ve ülke gerçeklerine göre farklılaşabilir. Her ne kadar dışarıdan danışmanlık desteği alınsa da risk yönetimi mevcut organizasyon yapısı içinde gerçekleştirilmelidir. Kurumun yapısına bağlı olarak risk yönetimi birimi yarı zamanlı risk yöneticisi ya da eksiksiz bir risk yönetim bölümü olabilir. Risk kültürüne göre risk yönetimi iç denetim birimi olarak ele alınabilir. Bu durumda iç denetim birimi objektif ve bağımsız bir şekilde çalışa bilmesi garanti altına alınmalıdır (IRM, 2010). Entegre risk yönetiminde ise tüm üst düzey şirket yöneticilerinin ve hatta bütün çalışanların bu süreçte önemli rolleri bulunmaktadır (Köksal, 2013).

Risk yönetimi içerisinde yönetim kademelerinin görev ve sorumlulukları net ve kapsamlı bir şekilde belirlenmelidir. Örneğin Yönetim Kurulu'nun şirketin risk eğilimini ve risk toleransını belirleme ve risk yönetimi içeriğini oluşturma sorumluluğu vardır. Risk yönetimi döngüsünde kontrollerin ve geriye dönük değerlendirmelerin yapılarak sürecin ve dolayısıyla şirketin risk yönetimi performansının geliştirilmesi gerekmektedir. Bu görev eğer varsa risk yöneticisine verilmektedir. Kısa bir şekilde risk yönetimine ilişkin görev ve sorumlulukları aşağıdaki gibi özetlemek mümkündür:

Tablo 11. Risk Yönetimi Görev ve Sorumlulukları

1. CEO ve Yönetim Kurulu'nun risk yönetimi sorumlulukları: Risk politikasını ve risk eğilimi ayarlama Risk yönetimi yapısını kurma En belirgin riskleri anlama Düzenli risk raporlarını analiz etme Organizasyonu kriz anında yönetme	**2. İş birimleri yöneticilerinin risk yönetimi sorumlulukları:** Birim bünyesinde risk bilinci kültürünü oluşturma Risk yönetimi performans hedeflerini belirleme Risk geliştirme tavsiyelerinin uygulanmasını sağlama Değişen durumları/riskleri belirleme ve raporlama
3. **Bireysel çalışanların Risk Yönetimi sorumlulukları:** Risk yönetim süreçlerini anlama, benimseme ve uygulama Verimsiz, gereksiz ya da çalışmaz kontrolleri raporlama Kaybedilmiş ve kaçırılmış olayları raporlama Kaza soruşturmalarında yönetimle koordineli hareket etme	**4. Risk yöneticisinin risk yönetimi sorumlulukları:** Risk yönetim politikasını geliştirme ve güncelleme İçsel risk politikaları ve yapılarının dokümantasyonu Risk yönetimi ve iç kontrol faaliyetlerinin koordinasyonu Risk bilgilerinin derlenmesi ve Yönetim Kurulu'na raporlanması
5. Uzman risk yönetim birimlerinin risk yönetimi sorumlulukları: Risk politikalarını kurmada şirkete yardımcı olma Acil durum ve kurtarma planları geliştirme Risk Yönetimi alanındaki yeni gelişmelerin adapte edilmesi Kaza ve benzer kayıp soruşturmalarını destekleme	**6. İç denetim yöneticilerinin risk yönetimi sorumlulukları:** Riske dayandırılmış iç denetim programı geliştirme Organizasyon bünyesindeki risk süreçlerini denetleme Riskin yönetiminde güvence alma ve temin etme İç kontrollerin verimliliği ve etkinliği üzerine raporlama

Kaynak*: KÖKSAL A. G*., 6102 Sayılı Türk Ticaret Kanunu Kapsamında Risklerin Tespiti Ve Yönetilmesin., e İlişkin Bağımsız Denetçinin Sorumluluğu*, C.Ü. İktisadi ve İdari Bilimler Dergisi, Cilt 14, Sayı 2, 2013.*

Etkin bir risk yönetimi için görev ve sorumluluklar dağılımı sürekli gözden geçirilmelidir. Gözden geçirmede, uyarlanan ölçülerle hedeflenen sonuca ulaşılıp ulaşılmadığı, uyarlanan prosedürlerin verimli olup olmadığı, risk

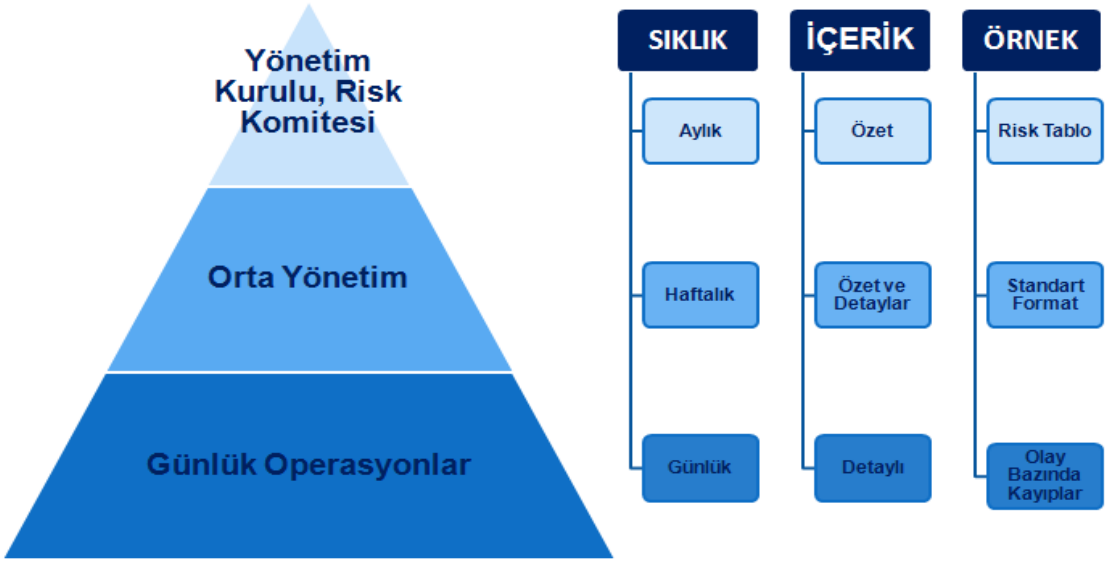
değerlendirmeleri için yeterli bilginin bulunup bulunmadığı, gelişmiş bilginin daha iyi kararlara ulaşmada yardımcı olup olmadığı, gelecekteki değerlendirmeler ve kontroller için ders alınıp alınmadığı açık ve net bir şekilde değerlendirilmelidir. Çıkan sonuçlara göre risk yönetimi süreci tekrar şekillendirilmelidir.

Tüm şirket kurul, bölüm ve birimlerinde yer alan herkesi kapsayan görev ve sorumluluk dağılımın yanında kurum içi iletişimin yaygınlaştırılması da önemli bir kurumsal risk yönetimi aracıdır. Karar vericilerden çıkar sahiplerine yapılabilecek karşı bilgilendirme yerine karşılıklı bir iletişim şeklinde şirket içi iletişim ağı kurulması gerekmektedir. Bu iletişim ortak platform (Kurumsal Raporlama Platformu, ERP) ve etkin bir raporlama sistemi ile gerçekleştirilebilir. Oluşturulacak raporlama sisteminde, risk yönetimine raporlarını gözden geçirip onaylayarak ile ilgili mercilere göndermesi ve rapor sonuçları takip ve kontrolü görevi verilerek, şirket içi iletişim de en yetkili merci olarak tanımlana bilir.

TTK 'da, denetçinin ve kurulacak risk komitesinin raporlarla üst yönetimi bilgilendirmesi zorunluluğu getirilmiştir. Uygulamada, TTK 'ya paralel olarak aşağıdan yukarıya doğru zorunlu raporlama olduğu, aynı derecede önem taşıyan aşağıya dönük iletişimin ise yeterli düzeyde olmadığı ya da hiç gerçekleşmediği görülmektedir. İletişimin yetersiz düzeyde olması süreç sahiplerinin üstlendikleri risklerin yeterince farkında olmamaları sonucunu doğurmaktadır (Topçu, 2010).

Kurumsal iletişim sadece kurum içinde değil aynı zamanda kurum dışındaki paydaşları da kapsamalıdır. Etkin bir kurumsal iletişim, şirket içi alınan kararların ve bunların sebeplerinin bütün menfaat sahipleri tarafından açık bir şekilde anlaşılması ve doğru uygulanması açısından oldukça önemlidir. Menfaat sahiplerinden etkin bir raporlama süreci ile elde edilen bilgiler, uygulamada ortaya çıkması olası risklerin hızlı bir şekilde tanımlanması, kayıt altına alınması ve karar alma sürecine entegre edilebilmesi için oldukça önemlidir. Karşılıklı görüş alışverişine dayalı bir takım yaklaşımı ortamını sağlayan platform oluşturulması ve rutin raporlama düzeneği kurulması, risklerin etkin bir şekilde

belirlenmesine, hızlı bir şekilde gerekli aksiyonların alınmasına yardımcı olacağı gibi, geri besleme süreci ile mevcut sistemin geliştirilmesini sağlayacaktır. Oluşturulacak rutin raporlama ve kurumsal iletişim platformu ile sadece yöneticilerin değil bütün menfaat sahiplerinin, riskleri ve risk yönetim süreçlerini daha iyi anlamalarını, sahiplenmelerini ve desteklemelerini sağlayacaktır (TÜSİAD, 2008). COSO risk yönetimi sürecinde yer alan örnek kurumsal raporlama sistemi aşağıda verilmiştir.



Şekil 11. Kurumsal Raporlama Sistemi

Kaynak: COSO, *Enterprise Risk Management*, https://www.coso.org, 2004

4. FİNANS DIŞI ŞİRKETLERDE KURUMSAL RİSK YÖNETİMİ UYGULAMASI VE RİSK MATRİSİNİN ÇIKARILMASI

4.1. Araştırmanın Amacı ve Önemi

Bu araştırmanın ana amacı, kurumsal risk yönetimi üzerine dünyadaki ve Türkiye'deki yasal uygulamalar ve uluslararası kabul görmüş risk yönetimi standartları üzerine niteliksel bir araştırma yapmak ve finans dışı sektörlerde kurumsal risk uygulamasının nasıl olması gerektiğini tartışmak, örnek vaka çalışması ile gerçekte nasıl uygulandığını göstermek ve örnek risk matrisini vaka çalışması ile elde edilen verileri kullanıma sunmaktır.

Artan ekonomik dalgalanmalar ve gittikçe kısalan iş döngüleri yüzünden sıklaşan krizler ve globalleşmenin etkisiyle artan kırılganlık kurumsal risk yönetimin önemini artırmıştır. Global ekonominin bir parçası olan ve gelişen ekonomilere özgü daha fazla kırılganlık taşıyan ekonomik ortamda Türkiye'deki şirketlerinde artık COSO tarafından standartları belirlenen ve ÇSGB tarafından geliştirilen rehberde[7] detayları yer alan risk matrisi çıkarılması ve buradan elde edilecek veriler üzerine oturtturulmuş entegre kurumsal risk yönetimi uygulamalarına geçmesini gerektirmektedir.

Kurumsal risk yönetiminin en önemli aracı olan risk matrisi hakkında farkındalığı artırmak ve uygulama örneği ile diğer finans dışı kurumsal firmalara yol göstermek amacıyla yakın zamanda hızlı büyüme göstermiş olan sanayi ve perakende alanlarında faaliyet gösteren bir şirketinin kurumsal risk yönetimi uygulaması incelenecektir. Elde edilen verilen ışığında COSO tarafından geliştirilen ve ÇSGB rehberinde yer alan risk matrisinin oluşturulması hedeflenmektedir.

[7] ÇSGB*, İç Kontrol Kurumsal Risk Yönetim Rehberi,* Strateji Geliştirme Başkanlığı, Ankara, 2013.

4.2. Araştırmanın Yöntemi ve Veri Toplama Araçları

Bu çalışmada kurumsal risk yönetimi uygulaması örneği ve risk matrisinin çıkarılması detaylı olarak aşamaları ile birlikte anlatılacaktır. Bir önceki bölümde teorik olarak açıklanan COSO Risk Yönetimi Uygulaması içeresinde yer alan Risk Değerlendirme Formu finans dışı sektörde önemli bir aktör olan bir şirketin üst düzey yöneticileri tarafından doldurulmuştur. Elde edilen sonuçlar değerlendirilerek örnek bir risk matrisi çalışması yapılmıştır. Bu araştırma da nitel bir araştırma deseni ve örnek olay yöntemi kullanılmıştır. Nitel araştırma, gözlem, görüşme ve doküman analizi gibi nitel veri toplama yöntemlerinin kullanıldığı ve bütünsel kıstaslarla incelendiği bir araştırma türüdür (Sığırı, 2018; Creswell, 2013; Yıldırım – Şimşek, 1999). Örnek uygulama ile daha önceki bölümlerde teorik olarak bahsedilen risk analizi, değerlendirilmesi ve sınıflandırılması konuları örnek olay üzerinden, gerçek veriler doğrultusunda somut bir temele dayandırılarak yapılması ve metin analizi yöntemi kullanılarak örnek bir risk matrisi oluşturulması hedeflenmiştir. İhtiyaç duyulan verilerin toplanması için COSO tarafından geliştirilen ve EK1'de yer alan Risk değerlendirmesi formundaki sorular yetkili üst düzey yöneticilerle yüz yüze görüşmeler sırasında doldurulmuştur. Ayrıca firmanın web sayfasından, hakkında çıkan gazete ve dergi haberlerinden ve ortaklarının PCW tarafından yapılmış ve yayınlanmış olan finansal dış denetim raporlarından belge inceleme yöntemi kullanılarak gerekli bilgiler toplanmıştır. Toplanan veriler, COSO, IRM ve ÇSGB tarafından yayınlanan risk yönetimi kılavuzlarında yer alan örnek olaylar ışığında metin analizine tabi tutularak risk matrisi hazırlanmıştır.

4.3. Araştırmanın Evreni ve Örneklemi

2001 yılı krizinden sonra bankacılık sektörünün yeniden yapılanması ve risk yönetimi uygulamasının yasa koyucu tarafından zorunlu hale getirilmesi yanında finans dışı sektörde henüz risk yönetimi olgunluğuna ulaşılmadığı görülmektedir. Bu doğrultuda araştırmanın evreni Türkiye'deki finans dışı işletmelerdir. Araştırmanın örneklemi sanayi ve perakende sektöründe faaliyet gösteren bir firmadır. Firmanın talebi üzerine ismi ve veriler açık olarak tezde kullanılmayacaktır.

4.4 Verilerin Analizi

Örnek olay için seçilen firmadan elde edilen bilgiler ışığında risklerin belirlenmesi[8], çıkma olasılıklarına ve oluşturacağı hasara göre derecelendirilmesi (ÇSGB, 2013) ve sıralanarak risk matrisine konulması için gerekli bütün veriler mülakat, gözlem ve doküman taraması gibi nitel araştırma teknikleri kullanılarak bulunmuştur. Risklerin değerlendirilerek skor verilmesi tezin 3. bölümünde detaylı bir şekilde verilen risk ölçme yöntemleri ile yapılmıştır. (Bakınız bölüm 3.2.7.5).

4.4.1. Risk Değerlendirme Formu

Risk tanımlama teknikleri içeresinde kullanılan risk değerlendirme formu esasında COSO (COSO, 2004) tarafından dizayn edilmiş, mevcut ve gelecekteki belirsizlikler hakkında şirketin kilit bölümündeki sorumlulardan oluşan grup çalışması olarak değerlendirilebilen, risk çalıştayının (risk workshop) bir parçasıdır. Risk çalıştayı sorunların ortaya çıkarılması, alınacak kararlar, gerçekleştirilecek eylemlerde sorumluluk paylaşımı konularının detaylı belirlenmesi için yapılmaktadır. Çalıştay mevcut durumdan çok gelecekle ilgilidir. Tüm bilinenlerin, ilgili durumların, varsayımların, belirsizliklerin bir araya getirilerek bunların firmanın hedeflerini nasıl etkileyeceği ve firmanın bunlarla nasıl başa çıkacağıyla ile ilgili kararlar asıl amaçtır. Çalıştayı istenildiği gibi yürütebilmek için COSO tarafından şirketin bütün önemli organlarını içeren bir risk değerlendirme formu geliştirilmiştir. Bu formdaki sorulara çalıştaya gelenler serbest bir ortanda tartışarak cevap vermeleri sağlanıp, verilen cevaplar ışığında riskler tanımlanıp olasılık ve etkileri belirlenerek risk matrisi çıkarılmak için kullanılır (Koltan, Orhon, Yılmaz, Altay, Çay, 2010).

4.4.2. Risk Matrisi

Veri analizi sonucunda ana amaç seçilen firmaya ait örnek bir risk matrisinin oluşturulmasıdır. Genel görüş olarak, risk belirleme çalışmaları sonucu ortaya çıkan kurumsal ve faaliyet risklerinin gerçekleşme olasılığı ile zaman, maliyet, performans ve itibar açısından etkileri bir araya getirilerek risk matrisi oluşturulur. En son ve en zor

[8] Firma faaliyetinin her aşamasında ortaya çıkan veya çıkabilecek risklerin yer aldığı kontrol listesi. (COSO, 2004)

olan bölüm de bu çıkan sonuçların arasında bağlantılar kurmaktır (ÇSGB, 2013). Risklerle ilgili etki ve olasılık değerlendirmesi 5'li ölçek (Tablo 12) kullanılarak ve objektif olarak yapılmaktadır. Türkiye'deki uygulamada risk analizi ve yönetimi bir ihtiyaçtan çok yasalara uyma zorunluluğu nedeniyle uygulandığı için en kolay uygulanabilen analiz yöntemi olan "Risk Değerlendirme Karar Matrisi" yaygın olarak kullanılmaktadır. Risk değerlendirme karar matrisi ABD askeri standardı olarak geliştirilmiş, 5x5 Matris diyagramı ile tehlikelerin oluşma olasılığı ile oluştuğunda meydana gelen zarar arasındaki ilişki analiz edilmek için kullanılmaktadır (Koltan, Orhon, Yılmaz, Altay, Çay, 2010).

5'li ölçek Tablo 12 dahilinde her bir riske çıkma olasılığı için bir değer verilir ve meydana getireceği etki için de yine aynı ölçekte bir değer verilir. Daha sonra bu iki değer çarpılarak risk için toplam risk skoru elde edilir. Elde edilen risk skoruna göre, riskler matris üzerinde 1x1=1'den 5x5=25'e kadar sıralanır ve gerekli aksiyonlar belirlenir (Güneş, 2009). Bilimsel olarak geçmiş veriler, olasılık dağılımları veya senaryo analizleri kullanılarak sayısal bir şekilde (kantitatif analiz) belirlenmesi gereken bu skorlar, veri ve teknolojik alt yapı eksikliğinden dolayı kalitatif bir şekilde geçmiş gözlemlere veya iş paydaşlarının deneyimlerine göre belirlenmektedir (Kuzucuoğlu, 2014).

Bulgular bölümünde yer alan risk matrisindeki risklerin nasıl skorlandığını örnek ile gösterecek olursak; uygulama yaptığımız firmada risk değerlendirme formu yardımıyla elde ettiğimiz önemli risklerden biri "Faturalardaki hatalar, vergi ödemeleri, SGK ve KDV (iadeleri) hesaplamalarında hatalar" olarak belirlenmiştir. Geçmiş tecrübelere göre bu riskin ortaya çıkma olasılığı 3 (orta sıklıkta ortaya gelecek bir sorun), meydana gelecek zarar (maliye tarafından verilecek cezalar) 4 (performansı büyük ölçüde etkileyen majör etki) ise, bu riskin risk skoru 3 x 4 = 12 olacaktır. Risk skoruna göre bu risk müdahale edilerek ve iç kontrollerle en aza indirilmesi gereken risk kategorisindedir.

Ortaya çıkan diğer önemli bir riske örnek verecek olursak, bulgular bölümünde detayları ile bahsedileceği gibi şirketin hızlı büyüme vizyonuna sahip oluğu ve bunun risk eğilimini artırdığını şirket hakkında toplanılan verilerden ve yapılan görüşmelerden belirlenmiştir. Dolayısıyla hızlı büyüme şirketin mevcut trendine göre 4 ortaya çıkma skoru ve hızlı büyümenin ve yüksek risk eğilimının ortaya çıkaracağı etki ise 5 skoru ile değerlendirilmiştir. Dolayısıyla risk skoru 4x5=20 olacaktır. Bu kesinlikle müdahale edilmesi gereken majör bir risktir ve şirketin kurumsallaşmaya önem vermesi ve vizyonunu tekrar gözden geçirmesi gerekebilecektir. Diğer önemli risk ülke ekonomisi olarak gösterilmiştir. Burada ülke ekonomisi ve tüm dünyada devam ekenomik dalgalanmalar bahsedilmektedir. Özellikle ülke ekonomilerindeki dalgalanmalar önceden hesaba katılarak risk sermayesi belirlenmesi önemlidir. Daha detaylı olarak şirket ile ilgili bilgilerin verildiği ve risklerle ilgili kalitatif analiz sonuçlarının yer aldığı bulgular bölümünde şirket riskleri değerlendirilmiştir.

Tablo 12'de ÇSGB tarafından yayınlanan risk yönetimi kılavuzuna göre riskin etkisinin ve çıkma olasılığının nasıl 5'li ölçek haline getirildiği gösterilmektedir.

Tablo 12. Etki Dereceleri ve Ölçeği

Puan	Derece	Etki		
		Zaman	Maliyet	Performans
5	yıkıcı	süreyi > %20 arttırır.	maliyeti > %20 arttırır.	performans kabul edilemez.
4	majör	süreyi %10-%20 arttırır.	maliyeti %10-%20 arttırır.	performansı büyük ölçüde etkiler.
3	orta	süreyi %5-%10 arttırır.	maliyeti %5-%10 arttırır.	performansı orta düzeyde etkiler.
2	minör	süreyi < %5 arttırır.	maliyeti < %5 arttırır.	performansı kısmen etkiler.
1	etkisiz	önemsiz süre artışı/etkisi yok	önemsiz maliyet artışı/etkisi yok	performansa etkisi önemsiz/etkisi yok

Kaynak: ÇSGB, *İç Kontrol Kurumsal Risk Yönetim Rehberi,* Strateji Geliştirme Başkanlığı, Ankara, 2013.

Tablo 13. Olasılık Dereceleri ve Ölçeği

Puan	Derece	Olasılık
5	çok büyük olasılıklı	gerçekleşme ihtimali çok yüksek (%80-%99)
4	muhtemelen	gerçekleşme ihtimali yüksek (%51-%79)
3	belki	herhangi bir şey söylenemez (%50)
2	az bir olasılıkla	gerçekleşme ihtimali düşük (%20-%49)
1	nadiren	gerçekleşme ihtimali çok düşük (% 1-%19)

Kaynak: ÇSGB, *İç Kontrol Kurumsal Risk Yönetim Rehberi,* Strateji Geliştirme Başkanlığı, Ankara, 2013.

Tablo 14. Örnek Risk Matrisi

RİSK MATRİKSİ ANALİZİ						
Etki	**1 Önemsiz**	**2 Az**	**3 Orta**	**4 Büyük**	**5 Çok Büyük**	**Olasılık Kategorisi Açıklama**
A. Hemen hemen kesin	5	10	15	20	25	A. Etkinin olması hemen hemen kesindir.
B. Çok Muhtemel	4	8	12	16	20	B. Etkinin olması çok muhtemeldir.
C. Muhtemel	3	6	9	12	15	C. Etkinin olması muhtemeldir.
D. Az Muhtemel	2	4	6	8	10	D. Etkinin olması az muhtemeldir.
E. Ender	1	2	3	4	5	E. Etkinin olması enderdir.

Kaynak: COSO, Enterprise Risk Management, https://www.coso.org, 2004.

4.5.Bulgular

Bu bölümde ilk önce şirket ile ilgili veriler risk yönetimi bakış açısı ile değerlendirilerek veril ve örnek risk matrisi oluşturulmuştur.

4.5.1. Şirket ve Sektörle İlgili Bulgular

1960 yılında küçük bir atölyede temelleri atılan şirket kendi tesislerinde 9700'ün üzerinde, bayilikleri ile birlikte 30.000'e yakın kişiye istihdam sağlamaktadır ve yılda 55 milyon çift ayakkabı satışı gerçekleştirmektedir. Şirkete bağlı olarak yurt içinde

550'e yakın mağaza, yurt dışında ise 14 ülkede 80'e yakın mağaza ile hizmet vermektedir.

Şirket kaliteli, sağlıklı, günün modasına uygun ayakkabıları yaygın satış ağı kurarak uygun fiyatlarla tüketicilere sunmak, kısaca herkesin ayakkabıcısı olmak misyonunu benimsemiştir. Bu misyonun altında Türkiye'de ayakkabı sektörüne öncülük etme ve sektörü dünya üretim liginde üst sıralara taşıma vizyonuyla hareket etmektedir. Bu vizyon doğrultusunda 2023 yılında Türkiye'den çıkacak 10 global markadan biri olmak hedefi koyulmuştur (Şirket Raporu, 2018). Dolayısıyla risk eğilimi bu vizyon ve hedef ile belirlenirken risk toleransları şirketin finansal ve kurumsal dinamikleri ile Türkiye'deki ekonomik ve politik çerçeve üzerinden ve hatta global ekonomik dalgalanmalar göz önüne alınarak belirlenmesi gerekmektedir.

2017 yılı itibariyle 2,6 milyar TL'lik ciroya ulaşan şirket 2018 yılı ilk yedi ayında yüzde 30 büyüme kaydetmiştir. Şirket stratejisi olarak, iç pazarda yaşanan konjonktürün getirdiği fırsatları değerlendirerek hem yurtdışında hem de yurtiçinde büyümesini sürdürmeyi belirlemiştir (Ekonomist, 2018). Ulaşılabilir fiyata ürün satmanın ve yurtiçi düşen kira fiyatlarının avantajından yararlanarak yüksek risk eğilimi ile stratejilerini belirledikleri ve yüksek büyüme hedefini sürdürebilmek için risk alma eşiklerini dalgalı konjonktüre rağmen oldukça yüksek tuttuklarını görülmektedir.

Şirket, 2023 yılı hedefine ulaşabilmek için 2012 yılında açılan Yeni Ayakkabı Fabrikasına ek olarak, 20 milyon TL toplam yatırım ile ikinci fabrikasını kurmayı planlamaktadır. İkinci fabrika yatırımı ile birlikte Güney Anadolu Bölgesindeki bir Organize Sanayi Bölgesinde, sektörel kümelenme (Clustering) modeli uygulayarak Ayakkabıcılar Sanayi Bölgesi kurulması için çalışmaktadır. 2015 yılında Kalite Laboratuvarı kurulmuş ve 2016'da Türkak Akredite belgesi alınmıştır. Kalite Laboratuvarı şu anda yıllık 240 bin ekolojik ve 10.000 fiziksel test kapasitesine sahiptir. Bu yatırım şirketin yurtiçi ve yurtdışında güvenirliğini artırdığı için önemli bir risk azaltma aksiyonu olarak görülebilir. 2013 yılında şirketin yüzde 50 hissesi, X Girişim A.Ş., Büyük Marketler Zinciri ve Mater Footwear BV konsorsiyumuna yaklaşık 500 milyon TL'ye satılmıştır (http://bigpara.hurriyet.com.tr /doviz/haber/turk-ayakkabi-devine-uc-yeni-ortak_ID897661). Oluşturulan dünya çapında marka olma ve yüksek büyüme stratejisini gerçekleştirmek ve yeni yatırımların finansmanını güçlendirilmek

için sermayesi güçlü yeni ortaklık önemli bir risk azaltma stratejisi olarak değerlendirilmektedir.

2015 yılında yurt dışında ilk mağazasını açan şirket, Avrupa'da büyüme hedefi doğrultusunda 2012 yılında İtalya'nın önemli bir ayakkabı markasını bünyesine katmıştır. Risk eğilimini belirleyen dünya genelinde yayılma ve 10 lider marka halline gelme hedefi doğrultusunda yatırımlar yapılmaya devam edilmektedir. İtalyan ayakkabı markasıyla Rusya'ya güçlü bir giriş yapmak için yatırımlarına devam eden şirket, aynı zamanda Fas, Kenya, Kongo Cumhuriyeti'nde de mağaza açmayı hedeflemektedir. Bu ülkelerdeki oynak ekonomik ve siyasi durum şirketin üstelendiği ülke riskini artırmaktadır. Önemli satış kanallarından olan e-ticareti yurtdışı satışlarında da güçlendirmek için e-ticaret entegrasyon projesi yürütülmektedir. Bu kapsamda Rusya, Romanya, Ukrayna başta olmak üzere yakın coğrafyaya hizmet veren birkaç uluslararası web sitesiyle e-ticaret sitesinin entegrasyonu sağlanarak e-ticaret performansı yükseltilmeye çalışılmaktadır. Şirket, 2023 yılı yurt dışı hedefleri doğrultusunda ihracatını 300 milyon dolara, yurtdışı mağaza sayısını toplam 47 ülkede 300'e ulaştırmayı ve Güneydoğu Anadolu Bölgesi'nde öncülük edilen organize sanayii yatırımları ile birlikte Türkiye'yi dünyanın en büyük ayakkabı üretim üslerinden biri yapmayı hedeflemektedir (Şirket Raporu, 2018).

4.5.2. Risk Değerlendirme Matrisi Sonuçları

Ek1'de yer alan COSO Risk Değerlendirme Formu şirket üst düzey yöneticilerine uygulanmıştır. Bu cevaplar kısaca aşağıda özetlenmiştir:

Firmanın misyonu "Kaliteli, sağlıklı, günün moda trendlerine uygun ayakkabıları yapıp, yaygın satış ağında uygun fiyatlarla müşterilerle buluşturarak herkesin ayakkabıcısı olmak" şeklinde tanımlamıştır. Firmanın hedefi 2023 yılına kadar Türkiye sınırları dışında kalıcı yer edinerek dünya çapında bir marka olmak diye sadece stratejik hedef tanımlanmış, operasyonel, raporlama ve finansal açıdan herhangi bir detay verilmemiştir.

Firmanın risklere karşı hızlı müdahale edecek şekilde yapılandığı ve risk yönetme konusunda yeterince yetkin olduğu söylenmiştir. Firma alınacak bir riskten doğacak potansiyel bir kaybı telafi edecek kapasiteye sahip olduğu belirtilmiş, risk

yönetimine firmanın bakış açısı "Operasyonun büyüklüğü nedeniyle maliyeti bizim için oldukça düşük olmasına karşın faydası oldukça yüksektir" şeklinde tanımlanmıştır.

Cevap veren muhasebe bölümünde çalıştığı için kendi bölümü ile ilgili kapsamlı bir risk yönetimi yapıldığını belirtmiştir. Buradaki risk yönetimi daha çok iç kontrol mekanizması üzerinde işlediği ve her ay sonu dönem kapanışlarında muhasebe sorumlusu olan kişilerin tüm hesapları tek tek kontrol ettiği ifade edilmiştir. En önemli risk, görevlerin tam olarak yerine getirilmemesi ya da eksik yerine getirilmesi sonucu, yasal ve regülasyon risklerinin içinde yer alan "yanlış işlemler nedeniyle vergi denetiminden yüksek bir ceza yeme ihtimali" olarak tanımlanmıştır.

En önemli risk olarak belirlenen yanlış işlem riskinin bertaraf edilmesi için tekrar iç kontrol mekanizmasına bağlı olarak önlem alınmakta ve kontrolün daha üst birimlere verilerek, dolayısıyla hiyerarşik bir yapıya bağlı kalınarak risk yönetimi yapıldığı söylenmiştir. Şirketin her departmanı taşıdıkları riskleri düzenli rapor haline getirip, bu raporları aylık hazırlayarak yönetime sundukları belirtilmiştir. Dolayısıyla yönetim kurulu riskleri sistematik bir şekilde aylık bazda hazırlanan raporlarla takip etmektedir.

Şirketin üst yönetim tarafından belirlenmiş bir risk stratejisi bulunmamakla birlikte riskleri sadece sigortalanabilen riskler olarak değerlendirilmeyip iç kontrol ve aylık raporlar üzerine kurulmuş statik bir risk yönetimi benimsenmiştir. Ara ve ana dönemli raporların etkin bir risk yönetimi sağlayarak olası risklere karşı çeşitli aksiyon ve reaksiyonlara yol açtığı belirtilmiştir. Aynı zamanda yönetimin, risk yönetimin bel kemiği olan raporlama sistemini, bilginin kalitesi, içeriğe uygunluğu, zamana uygunluğu, ulaşılabilirlik kesinlik gibi faktörlere göre değerlendirerek incelediği ifade edilmiştir.

Risk yönetimin ana direği olan iletişimin şirket içindeki portal ile hızlı ve etkin bir şekilde yapıldığı belirtilmiştir. Çalışanların riskleri ve sorunları bildirdikleri bu portal yardımıyla yönetim tarafından irdelenmesi gereken sorunlar ve riskler çalışanlar tarafından tam olarak anlaşılıp saptanabildiği ifade edilmiştir. İletişimin hızlı ve etkin olması için doğrudan ya da portal yardımıyla direk yönetici ile temasa geçile bilindiği söylenmiştir.

Çalışanların faaliyetlerini geliştirmelerini tavsiye eden bir mekanizma mevcut olup, yönetimin yapısal gelişimi, denetimi ve sağlamlığı sağlayacak tavsiyelere karşı açık olduğu söylenmiştir. Kurumun kendi etik kurallarından ve uygunsuz kabul ettiği davranışlar hakkında dış çevreyi (tedarikçiler ve 3. şahıslar) bilgilendirdiği, dış çevreden gelen şikayetlerin gerekli yönetim kademeleri tarafından dikkate alındığı ve sorunlarla ilgili kontroller yapıldığı belirtilmiştir.

Şirket organizasyon şemasını güncel olmadığı için paylaşılmamıştır. Halka açık bir şirket olmadığı için TTK 'ya göre risk yönetimi kurulu kurulması zorunluluğu getirilmediği için risk ile ilgili ayrı bir oluşum olmayıp, direk yönetim kuruluna bağlı iç denetim departmanı bulunmaktadır. Aylık her bölümün ayrı ayrı hazırladığı raporlar direk yönetim kuruluna sunulmaktadır. Aynı zaman da dış denetim olarak da hem Türk hem de yabancı denetim firmaları tarafından finansal denetim yapılmaktadır. Yabancı denetim şirketi olarak PWC şirketinin adı verilmiş ama herhangi bir denetim raporu paylaşılmamıştır. Şirketin operasyonel risk için acil eylem planı olduğu belirtilmiş ama paylaşılması uygun bulunmamıştır.

Bu bulgular ışığında incelenen firmanın risk değerlendirme matrisi oluşturulmuş ve aşağıda yer alan tablo 16'da sunulmuştur.

Tablo15. X Şirketi Örnek Risk Matrisi Uygulaması

	Finansal Risk	**Olma Olasılığı**	**Etkisi**	**Risk Skoru**	
1	Ödemede problemler	2	2	4	Kontroller artırılarak müdahale edilmeli
2	Satışların azalması	3	4	12	Mümkünse transfer edilmeli ya da yeni pazarlara gidilmesi
3	Likidite ve finansman riski	3	3	9	Mümkünse banka hizmetleri kullanılarak transfer edilmeli
4	Bilançolardaki hatalar	3	3	9	Kontroller artırılarak müdahale edilmeli
5	Yeni projelerin finansmanı	3	3	9	Banka hizmetleri kullanılarak müdahale edilmeli
6	Kredi, faiz ve döviz riski	4	5	20	Para piyasası enstrümanları kullanılarak ortadan kaldırılmalı
	Operasyonel Riskler				
7	Duygusal kararlar alınması (Kurumsallık Eksikliği)	4	4	16	Kurumsallaşma sağlanarak ortdan kaldırılmalı
8	Geleneksel yapının kurumsal yapıdan önce gelmesi	2	3	6	Kurumsallaşma sağlanarak müdahale edilmeli
9	İş güvenliği riski (fabrika, depo, vs)	2	2	4	İş Güvenliği Risk Yönetmeliğinin tam uygulanması ile müdahale edilmesi
10	ERP programı kullanımının azlığı	3	4	12	Uygulamanın yaygınlaştırılması için müdahale edilmesi
11	Görev tanımlarının tam olmaması	4	4	16	Kurumsallaşma ile ortadan kaldırılması
12	İç kontrol ve denetim mekanizmasındaki aksaklıklar	3	4	12	Kontrol mekanizması artırılarak müdahale edilmesi veya dış denetim firmasına transfer edilmesi
13	Makine ve ekipman arızaları (yurtdışından geldikleri için, servis sıkıntısı)	2	2	4	Prosedürlerin tam belirlenmesi ile müdahale edilmesi
14	E-ticarette teknolojik alt yapı ve dolandırıcılık işlemleri	4	3	12	Başka bir teknoloji şirketine transfer edilerek müdahale edilmesi
15	Sürekli çalışılmayan özel malzemeler	3	2	6	Deneyimli elemanlar istihdam edilerek müdahale edilmesi
16	Şirketin hızlı büyümesi	4	5	20	Kurumsallaşma sağlanarak iflas riskinin ortadan kaldırılması

17	Tedarikçiden gelen aksaklıklar	5	5	25	Detaylı bir tedarik kontrol sistemi uygulaması ile ortadan kaldırılması
18	Nitelikli personel bulma sıkıntısı	3	4	12	Fabrikaların bulunduğu bölgeye göre iç eğitim ile personel yetiştirilmesine önem verilerek müdahale edilmesi
19	Ürün kalitesi, malzeme riski	2	3	6	Kalite kontrol prosedürleri ile müdahale edilmesi
	Uyma/Uyum Riski				
20	Sicil kayıtları (SGK ödemelerindeki maddi hatalar şirketin siciline işleniyor.)	4	5	20	Kontrol mekanizmalarına önem vererek ortadan kaldırılması
21	Faturalardaki hatalar, vergi ödemeleri, ve KDV (iadeleri) hesaplamalarında hatalar	3	4	12	Kontrol mekanizmalarına önem vererek müdahale edilmesi
	Stratejik Risk				
22	Ülke ekonomisi riski	4	5	20	Mevcut ekonomik duruma göre riskli kararların ertelenmesi
23	Planlamadaki eksiklikler, plan ve öncelik sınıflandırmasının yapılmaması	4	4	16	Kurumsallaşma sağlanarak ortadan kaldırılması
24	İç ve dış siyasi dinamiklerin, politik ve siyasi hareketlerin değişmesi	4	4	16	Mevcut dış çevre analizi yapılarak ya da bu konuda danışmanlık alınarak riskli kararların ertelenmesi
25	Proje tasarımındaki hatalar	4	5	20	Kurumsallaşmanın sağlanması ile ortadan kaldırılması
26	Güçlü Rakipler	5	5	25	Mevcut uluslararası rakiplere karşı güçlü tsratejiler geliştirerek ortadan kaldırılması

Toplam Skor 15-25: Ortadan kaldırılmalı

Toplam Skor: 8-12: Mümkünse transfer edilmeli ya da müdahale edilmeli

Toplam Skor 4- 6: Müdahale edilmeli

Toplam Skor 1-3: Kabul (Tolere) edilebilir.

Kaynak: Yazarın kendisi, COSO, Enterprise Risk Management, https://www.coso.org, 2004

Tartışma

Elde edilen ve elde edemediğimiz bilgiler ışığında şirketin çok hırslı bir vizyona ve buna bağlı olarak yüksek hedeflere sahip olduğu, bu yolda aşırı büyümeci bir politika sürdürdüğü, fakat bu büyümeyi sürdürebilmek için gerekli kurumsallaşmanın sağlanamadığı görülmektedir. Daha önceki bölümde de belirttiğimiz gibi şirket yönetimi belirlediği" 2023'te dünya çapında tanınmış global markalardan biri olmak" ve "yaygın bir mağazacılık ve e-ticaret ağı ile dünya geneline yayılmak" gibi yüksek hedefler doğrultusunda yüksek risk eğilimi ile çalışmakta fakat kurumsal risk yönetimi yapmamaktadır. Kurumsal risk yönetimi yerine daha ilkel iç denetime bağlı (internal audit), aylık alttan üste doğru raporlama aracılıyla statik bir risk yönetimi yapıldığı görülmektedir. Şirket içinde portal yönetimi ile iletişimin hızlandırılmış olması önemli bir risk indirgeme metodu olarak görülebilir. KRY'nin önemli bileşeni olan ERP uygulaması olarak kabul edebileceğimiz bu portalın ne kadar etkin bir şekilde çalıştığına dair elimizde bir veri bulunmamaktadır. Risk yönetimi kapsamında Şirketin operasyonel riskler için acil eylem planı olduğu belirtilmiştir.

Şirketin risk yönetimindeki en önemli eksiği dış iletişim olarak görülebilir. Ne resmi şirket web sayfasında ne de şirket ile iletişime geçildiğinde şirketin organizasyonel yapısı hakkında bilgi vermektedir. Bir şirketin omurgasını oluşturan organizasyon şemasının güncel olmadığı için paylaşılmamış olması şirket içi görev ve sorumlulukların tam bir şekilde belirlenmemiş olduğunu göstermektedir. Oysa risk yönetiminin en önemli gereksinimi şirket içinde görev ve sorumlulukların tam ve eksiksiz bir şekilde tanımlanmasıdır. Ayrıca şirketin web sayfasındaki iletişim bilgilerinin bile yanlış olması, yatırımcı ilişkileri dahil şirketin dışarıya karşı kapalı olduğunu göstermekte ve risk yönetiminin önemli bir elemanı olan şeffaflık ilkesi yok sayılmaktadır. Şirketin faaliyet raporu ve dış denetim raporunu paylaşmak istememesi de aynı şeye işaret etmektedir.

Şirketin büyümek için 2013 yılında yaptığı sermaye katılımının büyük bir bölümünün X Girişim Ortaklığı A.Ş. ve Büyük Marketler Zinciri tarafından yapılması şirketin iç siyasi destek ile güçlenen yeni ekonomik aktörlerden biri olduğu göstermektedir. Mevcut siyasi otoriteye yakınlık, kurumsal yapısı güçlü olmayan ve gelişmekte olan ekonomilerdeki pazar yapısına sahip olan Türkiye standartlarında önemli bir ivme verici etken olmakla birlikte, şirketi siyasi çalkantılara açık bir hale

getirmektedir. Aynı zamanda şirketin %11,5'ine sahip olan X Girişim'in Türkiye ekonomisindeki dalgalanmalara bağlı olarak 2017 ve 2018 yıllarında zarar açıklamış olması şirket risk toleranslarını belirlemek için gerekli olan risk sermayesini önemli ölçüde ters etkilemektedir (PWC, 2017). Risk toleransları azalırken risk eğilimının da bu azalma trendine uydurulması ve hedeflerin tekrar gözden geçirilmesi önemlidir. Elde edebildiğimiz tek şirket içi rapor olan "Satın Alma Departmanı 2019 Hedef Bütçe Raporu"na göre şirketin %64 bütçe tasarrufu ve %24 proje tasarrufuna gittiği görülmektedir. Satın alma bölümü de 2019 yılı için daha çok idari satın alma tasarrufuna gitmeyi planlamaktadır. Bu hedefler gittikçe zorlaşan konjonktüre bağlı olarak şirketin risk toleransında bir azalma olduğunu ve buna bağlı olarak risk eğilimında da azalma olduğunu göstermektedir.

2012 yılında açılan ilk Ayakkabı Fabrikasına ek olarak, 20 milyon TL toplam yatırım ile ikinci fabrikasını kurmayı planlanması, 2015 yılında Kalite Laboratuvarı kurulmuş ve 2016'da Türkak Akredite belgesi alınmış olması ve Avrupa'da büyüme hedefi doğrultusunda 2012 yılında İtalyan ayakkabı markasını bünyesine katması önemli sermaye birikimi isteyen adımlardır. Fabrika ve kalite laboratuvarı şirketin dikey entegrasyon ile üreticiden gelen riskleri ve Avrupa pazarında doğacak kalite risklerini azaltmak için atılmış risk azaltıcı faaliyetler olarak görülebilir. İtalyan ayakkabı markasının alınması da dış pazarlarda Türk markasının yarattığı negatif etkiyi bertaraf eden bir risk azaltma adımı olarak görülebilir. Fabrika'nın Güneydoğu Anadolu Bölgesi'nde kurulması yatırım teşviki alınması ve ucuz girdi sağlanması açısından önemli bir aksiyon olarak görülmelidir. Bununla birlikte şirketin misyonunun "Fiyatları uygun seviyede tutarak herkesin ayakkabıcısı olmak" olduğu düşünüldüğünde, Çin, Bangladeş, Pakistan gibi maliyetlerin daha da ucuz olduğu ülkelerdeki yüksek kapasitedeki üretimin önemli bir rekabet riski oluşturduğu görülmektedir.

Risk matrisinde yer alan riskler daha önceki bölümde bahsedildiği gibi şirket üst düzey yöneticileri ile yapılan görüşmeler, şirket hakkında elde edilen bilgiler ve risk yönetimi literatüründe yer alan örnek olaylarda yer alan riskler göz önüne alınarak belirlenmiştir. Olasılık ve etki puanları yine yapılan görüşmeler ve diğer örnek olaylardaki puanlamalar göz önüne alınarak nitel bir analiz ile oluşturulmuştur. Olasılık ve etki puanları çarpılarak risk skoru oluşturulmuştur.

Örnek risk matrisinin sonucunda şirketin öncelikle kurumsallığa önem vermesi ve bu konuda acil adımları atması gerekmektedir. Kurumsallaşmanın ve risk kültürünün yerleşmesi ve şirketin entegre bir şekilde kurumsal risk yönetimine geçebilmek için gerekli yapılanmayı sağlayıp, şirket içi eğitime önem vermesi gereklidir. Aynı zamanda şirketin vizyonunu kuracağı entegre risk yönetimi uygulamasına göre tekrar gözden geçirmesi, buna göre risk eğilimini daha niteliksel yöntemlerle test edip yeniden belirlemesi son derece önemlidir. En son olarak şirketin yüksek risk eğilimine bağlı olarak yüksek risk sermayesi oluşturması ve bu yönde başka finansal ortaklıklar bulması önemli bir adım olarak görülebilir.

SONUÇ

Giriş bölümünde de belirtildiği gibi bu tez zor ekonomik koşullar çerçevesinde artan kurumsal risk yönetiminin önemine dikkat çekmek amacıyla yazılmıştır. Tezin içerisinde risk yönetimi ile ilgili teorik bilgiler, Türkiye'deki yasal düzenlemeler ve finans dışı sektörden hızlı büyüyen bir şirketten elde edilen bilgiler temel alınarak yapılan risk matrisi uygulaması yer almaktadır. Birinci bölümde risk, kurumsal risk yönetimi ve bileşenleri olan kurumsal yönetim ve iç denetim hakkında teorik bilgi verilmiştir. Kurumsal risk yönetimi, şirketin karşılaştığı risklerle ilgili objektif prosedürlerin oluşmasını, şirket organizasyonunda herkesin görev ve sorumlulukları kesin bir şekilde tanımlanmasını ve şirket içi ve dışı gerekli bilgiye gerekli kişilerin hızlıca ulaşmasını sağlayan iletişim alt yapısını oluşmasını sağladığı için, şirket yönetiminin uluslararası standartlara oturttuğu için şirket yönetimini güçlendirmektedir.

Araştırmalar sonucu halka açık olmayan finans dışı şirketlerin risk yönetimi konusunda yetersiz oldukları görülmüştür. Aynı zamanda yeni TTK risk yönetimine ilişkin maddeleri genellikle organizasyonel yapı ve iç denetim unsurlarını ön plana çıkarmak ile birlikte risk yönetimini nasıl yapılması gerektiğine ilişkin bir yöntem vermemiştir. TTK'nin hakla açık olmayan şirketlerde bağımsız bir risk kurulu oluşturma zorunluluğu bile getirmemesi göz önüne alındığında, risk yönetiminin iç denetimden bağımsız düşünülmesi şu aşamada mümkün gözükmemektedir. Fiziki riskler için Avrupa Birliği ve uluslararası taahhütler doğrultusunda geliştirilen ve yasalaşan İş Sağlığı ve Güvenliği Kanunu ve birlikte çıkan yönetmeliklerde koruyucu ve iyileştirici bir anlayış benimsenmiştir. Kanun ve yönetmelik risk değerlendirilmesini daha çok işin fiziki yapılma koşullarına ve şekli kapsamında sınırlı bir yapıda tutmuştur. Kanun ile getirilen yaptırımlar iş kolundaki tehlike sıralamasına göre zorunlu hale getirilmiştir. İş kaza istatistikleri doğrultusunda yapılan analizde belirtildiği gibi eksikler vardır. Uygulamanın yaygınlaşması ve risk kültürü oluşturulması ancak, şirket içi veya dışı eğitim ve kanun yapıcının yaptırımları artırması ile oluşturula bilir. Risk yönetiminin riskleri azaltma bakış açısından çıkarılıp, fırsat yönetimi haline getirebilmek için sürecin her kademesi belli bir öğrenme, araştırma, hesaplama ve uygulama evresini içermelidir.

Risk değerlendirme formu sonuçları verilerine göre şirketin risk matrisi çıkarılmıştır. Şirketin iç denetim departmanı aracılığıyla risk yönetimi yaptığı tespit edilmiş olup henüz şirket içi risk kültürünün oluşmadığı görülmüştür. Şirketin yüksek stratejik hedeflerine ulaşması için şirketin daha kurumsallaşması ve risk yönetimine daha fazla önem vermesi gerektiği düşünülmektedir.

Şirketin, entegre kurumsal risk yönetimi uygulamasına geçmek için gerekli alt yapıyı hazırlaması gerekmektedir. Bunun için uzman personel istihdam edilmesi, şirket içi organizasyonun şirket dışındakilerle hızlı bir şekilde paylaşabilecekleri şekilde de daha şeffaf hale getirilmesi, şirket içi eğitimler düzenlenerek sürdürülebilir bir büyüme için gerekli olan risk yönetiminin iç denetim dışına çıkarılıp şirketin işleyişinin her aşamasına entegre edilmesi önemlidir. Özellikle gittikçe zorlaşan ekonomik şartlar ve küresel piyasalardaki hızlı dalgalanmalar göz önüne alınarak, şirketin stratejik hedeflerinin yeni gelişmelere adapte edilmesi gerekmektedir. Şirket ve risk yönetimine daha bilimsel bir bakış açısıyla bakılması ve değişen dışsal çevreye göre stratejik hedeflerin daha belirgin hedefler haline getirilmesi şirket açısından önemli bir adım olacaktır.

KAYNAKÇA

AŞÇI, B., *Olasılık Yönetimi: Senaryo Analizi,* 21. Yüzyılda Eğitim ve Toplum Dergisi, Cilt 6, Sayı 17, http://dergipark.gov.tr/download/article-file/436710, 2017.

BABUŞCU, Ş., *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi*, Akademi Consulting &Training, Ankara, 2005.

COSO, Enterprise Risk Management, https://www.coso.org, 2004

ÇELİKTAŞ, B., *Risk Değerlendirme Karar Matrisi Yöntemi Kullanarak Örnek Bir Risk Değerlendirme,* https://www.researchgate.net/publication/323835777, 2018.

ÇSGB*, İç Kontrol Kurumsal Risk Yönetim Rehberi,* Strateji Geliştirme Başkanlığı, Ankara, 2013.

ÇSGB, *6331 Sayılı İş Sağlığı ve Güvenliği Kanunu,* T.C. Çalışma ve Sosyal Güvenlik Bakanlığı Genel Yayın No: 52, Ankara, 2016.

EMHAN, A., *Risk Yönetim Süreci ve Risk Yönetmekte Kullanılan Teknikler*, Atatürk Üniversitesi İ.İ.B.F., Sayı:3, Cilt 23; 209-220, 2009.

ERDİKLER, Ş., http://Ww.Turmob.Org.Tr/Turmob/Basin/22-01-(4).html, 2003.

EWF, *Fundementals of Risk Management*, http://www.dphu.org/uploads/ attachements/books/books_3631_0.pdf, 2008.

FERMA, *Avrupa Risk Yönetimi Dernekleri Federasyonu Risk Yönetimi Standarttı*, https://www.ferma.eu/, 2002.

EKONOMİST, *2019'da yurtdışında 40 mağaza açacak*, www.ekonomist.com.tr/, 2018.

GÜNEŞ, Ş., *Kurumsal Risk Yönetimi ve Türkiye'de Farkındalığına İlişkin Bir Uygulama,* İTÜ İşletme Mühendisliği Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2009.

IRM, *Kurumsal Risk Yönetimine (KRY) Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri,* AIRMIC, ALARM, IRM, 2010.

KAŞIKÇI, F., *Risk Odaklı Denetim ve Bir Uygulama*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2006.

KİMBROUGH, R.L., COMPONATİON, P. J., *The Relationship Between Organizational Culture and Enterprise Risk Management,* Engineering Management Journal, 21:2, 18-26, UK, 2009.

KOLTAN, A., ORHON, Y., YILMAZ, S., ALTAY, M., YILMAZ, S., ÇAY, İ., *Risk Değerlendirmesinde Kullanılan L Tipi Karar Matrisi Yönetiminin İşçi Sağlığına Uygunluğunun Değerlendirilmesi*, TBB Mesleki Sağlık ve Güvenlik Dergisi, İstanbul, 2010.

KÖKSAL A. G., *6102 Sayılı Türk Ticaret Kanunu Kapsamında Risklerin Tespiti Ve Yönetilmesin., e İlişkin Bağımsız Denetçinin Sorumluluğu,* C.Ü. İktisadi ve İdari Bilimler Dergisi, Cilt 14, Sayı 2, 2013.

KUZUCUOĞLU, A.H., *Risk Management in Libraries, Archives and Museums,* IIB International Refereed Academic Social Sciences Journal, Sayı: 15 Cilt: 5, 2014.

KÜÇÜKÖZMEN, C.C., *Yeni Türk Ticaret Kanunu ve Risk Yönetimi,* Ekonomik Çözüm Gazetesi, http://www.coskunkucukozmen.com /wp-content /uploads /2012/05/ yenittkveriskyonetimicoskunkucukozmen.pdf, 2012.

MİCCOLİS, J., ERM Lessons Across Industries, http://www.irmi.com/ Expert/Articles/2003/Miccolis03.aspx, 2003.

MERİT RİSK YÖNETİMİ VE DANIŞMANLIK, *Kurumsal Risk Yönetimi ve Uygulaması,* İstanbul 2012.

OECD, *G20/OECD Principles of Corporate Governance"*, OECD Publishing, Paris, 2016.

OLSSON, C., *Risk Management in Emerging Markets,* Pearson Education Limited, UK., 2002.

PRİCEWATERHOUSECOOPERS, *Her Yönüyle Kurumsal Risk Yönetimi*, PWC, Infomag Yayıncılık, 2006.

PRİCEWATERHOUSECOOPERS, *X Girişim A.Ş. Dış Denetim Raporu*, 2017

RESMİ GAZETE, Sayı: 28339, Kanun No: 6335, *6102 sayılı TTK ile 6103 sayılı TTK Yürürlüğü ve Uygulama Şekli Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun*, 2012.

RESMİ GAZETE, Sayı: 28512, *İş Sağlığı ve Güvenliği Risk Değerlendirmesi Yönetmeliği*, 2012.

RESMİ GAZETE, Sayı: 28552, Karar No: 4151, *İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik*, 2012.

RİSK YÖNETİCİLERİ DERNEĞİ, *Basel II ve Basel II Nedir?*, Basel II ve Türk Eximbank Semineri, 2013.

SIĞIRI, Ü. *Nitel Araştırma Yöntemleri,* İşletme-Ekonomi Dizisi: 964, Asya Basım Yayın Sa. Tic. Ltd. Şti, İstanbul, 2018.

SGK, *İş Kazası ve Meslek Hastalıkları İstatistikleri,* http://www.sgk.gov.tr, 2017.

ŞİRKET, *Kurumsal Raporlar*, http://kurumsal.flo.com.tr/, 2018.

T.C. ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI, *Risk Değerlendirme Talimatı,* KYS-TLM-102, 2018.

TOPÇU, B., *Finans Dışı Şirketlerde Kurumsal Risk Yönetimi,* Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi, İstanbul, 2010.

TÜSİAD, *Kurumsal Yönetim İlkeleri*, Lebib Yalkın Yayımları ve Basım İşleri A.Ş., İstanbul, 2000.

TÜSİAD, *Kurumsal Yönetim En İyi Uygulama Kodu: Yönetim Kurulunun Yapısı ve İşleyişi*, Lebib Yalkın Yayımları ve Basım İşleri A.Ş., İstanbul, 2002.

TÜSİAD, *Kurumsal Risk Yönetimi*, Lebib Yalkın Yayımları ve Basım İşleri A.Ş., İstanbul, 2008.

EKLER

Ek-1: COSO Risk Değerlendirme Formu

Başlangıç soruları:

1.Firmanın risklere karşı yaklaşımı ne nasıldır?

2.Firmanın hedefleri nelerdir?

3.Firma riskleri yönetme konusunda ne kadar yetkindir?

4.Firma alınacak bir riskten doğacak potansiyel bir kaybı telafi edecek kapasiteye sahip midir?

5.Riskleri yönetmenin maliyeti ve faydaları nelerdir?

Risk Değerlendirmesi Soruları				
Sorular	Evet	Hayır	Cevap yok	Durumun kaynağı & Durumla ilgili ek bilgi
Bölümünüz risk değerlendirmesi yapıyor mu? Eğer yapıyorsa, bu değerlendirmeyi kapsamlı ve tam olarak nitelendirebilir misiniz?				
▪ Departman, proje veya aktiviteler için oluşturulan gruplar (ekip çalışması) faaliyet, amaç ve fonksiyonlarına göre gerçekçi bir yaklaşımla ve bir kontrol döngüsü içerisinde analiz ediliyor mu?				
▪ Her döngüyü fonksiyon ve aktiviteleriyle beraber listeleyiniz.				
▪ Daha önce deneyimlediğiniz riskleri, potansiyel problemleri ya da her bir aktiviteyle ilgili zayıflıkları betimleyiniz.				
▪ Bu zayıflıkları keşfetmek için ve hararetlenmesini önlemek için çeşitli kontroller yapılıyor mu?				
Değerlendirin : o Belirli bir riskin ortaya çıkma ihtimali? o Belirli bir riskin etkisi ve önemi?(eğer riskten başarıyla kaçınılamazsa, riskten dolayı ortaya çıkan zararın derecesi)?				
▪ Belirli bir riskin çıkma ihtimalini ve önemimi baz alarak durumu düzeltici bir hareket belirtin?				
▪ Şirketinizin her departmanı, departman olarak taşıdıkları riskleri düzenli bir şekilde rapor haline getiriyor mu?				
▪ Getiriyorsa bunu ne sıklıkta gerçekleştiriyor ve bu rapor şirkette hangi birime yollanıyor? Getirmiyorsa, departman risklerinin belirlenmesi için bir aksiyon alınıyor mu?				
▪ Bu raporlar konsolide bir şekilde yönetim kademesine ve oradan yönetim kuruluna yollanıyor mu? Ne kadar sürede bir yollanıyor?				
▪ Yönetim kurulu şirket risklerini sistematik bir şekilde takip edip, raporunu talep ediyor mu?				
▪ Şirketinizde üst yönetim tarafından belirlenmiş bir risk stratejisi var mı?				
▪ Riskleri sadece sigortalanabilen riskler olarak mı değerlendiriyorsunuz?				
▪ Şirketinizin misyonu, vizyonu nedir?(Üst kademeye sorulacak.)				
▪ Şirketin hedefleri nedir? (Stratejik, operasyonel, raporlama, finansal açılardan) (Üst kademeye sorulacak.)				

Mülakat				
Sorular	Evet	Hayır	Cevap Yok	Durumun kaynağı & Durumla ilgili ek bilgi
• Ara ve ana dönem raporları, faaliyetlerin ve işlemlerin etkili biçimde gözlemlenmesini sağlıyor ve çeşitli reaksiyon ve aksiyonlara yol açıyor mu?				
• Yönetim rutin bir şekilde raporlanmış bilginin kalitesini; içeriğe uygunluk, zamana uygunluk, ulaşılabilirlik, kesinlik gibi faktörlere göre değerlendirerek inceler mi?				

Mülakat				
Sorular	Evet	Hayır	Cevap Yok	Durumun kaynağı & Durumla ilgili ek bilgi
Yönetim, şirket içi iletişimin etkili bir şekilde oluşmasını sağlar. İrdeleyin:				
• Çalışanlar için iletişime geçtikleri / şüphelenilen ya da algılanan yanlışlıkları, riskleri ve sorunları bildirdikleri bir kanal /birim mevcut mudur?				
• Yönetim tarafından irdelenmesi gereken sorunlar ve riskler çalışanlar tarafından tam olarak anlaşılmakta, saptanabilmekte midir?				
• Kurumdaki iletişim zinciri bir kişi aracılığıyla mı gerçekleşiyor yoksa doğrudan yöneticiyle iletişime geçilebiliyor mu?				
• Çalışanların faaliyetlerini geliştirmesini tavsiye eden bir mekanizma mevcut mu? Yönetim yapısal gelişimi, denetimi ve sağlamlığı sağlayacak tavsiyelere karşı açık mı?				
Yönetim şirket dışı çevreyle iletişimi sağlamalıdır. İrdeleyin:				
• Kurum kendi etik kurallarından ve uygusuz kabul ettiği davranışlardan(örneğin: uygunsuz finansal işlemler) dış çevreyi (örneğin: tedarikçiyi) bilgilendiriyor mu?				
• Dış kaynakların şikâyetleri gerekli yönetim kademeleri tarafından dikkate alınıyor ve sorunla ilgili kontroller yapılabiliyor mu?				

Bilgi ve İletişim _____ Yeterli _____ Yetersiz

ÖZGEÇMİŞ

23 Ağustos 1989 yılında Iğdır'da doğdum. İlk, orta ve lise eğitimi Iğdır Merkez ilçede tamamladım. Üniversite hayatına 2011 yılında Beykent Üniversitesi, Lisans İktisat bölümünü kazanarak başladım. 2015 yılında mezun oldum. Daha sonra ise babamın şirketinde müdür yardımcısı olarak işe başladım. 3 yıl babamın şirketinde tecrübe edindikten sonra kendi işimi kurmak için işten ayrıldım. Şuan için serbest meslek ile uğraşmaktayım. 2018 yılında, Beykent Üniversitesi, İşletme Anabilim Dalı İşletme Yönetimi bölümünde yüksek lisans eğitimine başladım.

Özel ilgi alanlarım, seyehat etmek, kitap okumak ve finans üzerine dergi ve gazeteler takip etmekteyim.

Hüseyin AĞGÜL