T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE DENETİMİ BİLİM DALI

ANONİM ŞİRKETLERDE RİSK YÖNETİM ARACI OLARAK İÇ DENETİM SİSTEMİ

Yüksek Lisans Tezi

AYTUNÇ YILDIRIM

İstanbul, 2013

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE DENETİMİ BİLİM DALI

ANONİM ŞİRKETLERDE RİSK YÖNETİM ARACI OLARAK İÇ DENETİM SİSTEMİ

Yüksek Lisans Tezi

AYTUNÇ YILDIRIM

Danışman: PROF.DR. NURAN CÖMERT

İstanbul, 2013

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

TEZ ONAY BELGESİ

İŞLETME Anabilim Dalı MUHASEBE DENETİMİ Bilim Dalı TEZLİ YÜKSEK LİSANS öğrencisi AYTUNÇ YILDIRIM'nın ANONİM ŞİRKETLERDE RİSK YÖNETİM ARACI OLARAK İÇ DENETİM SİSTEMİ adlı tez çalışması, Enstitümüz Yönetim Kurulunun 28.06.2013 tarih ve 2013-24/17 sayılı kararıyla oluşturulan jüri tarafından oy birliği / ~~oy çokluğu~~ ile Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi ...19.../...07.../..2013...

Öğretim Üyesi Adı Soyadı			**İmzası**
1.	Tez Danışmanı	Prof. Dr. NURAN CÖMERT	
2.	Jüri Üyesi	Doç. Dr. FATMA PAMUKÇU	
3.	Jüri Üyesi	Doç. Dr. ÖZGÜR ÇATIKKAŞ	

GENEL BİLGİLER

İsim ve Soyadı : Aytunç YILDIRIM

Anabilim Dalı : İşletme

Programı : Muhasebe Denetimi

Tez Danışmanı : Prof. Dr. Nuran CÖMERT

Anahtar Kelimeler : Risk, Risk Yönetimi, Kurumsal Yönetim

ÖZET

Artan rekabet düzeyi, Anonim Şirketlerde gerçekleşen ürün ve hizmetler yoğunluğu risklerin gerçekleşme olasılığını ve kurumlarda kayıpların etkisini arttırmıştır. Meydana gelen büyük kayıplar ve skandallar risk yönetiminin gelişmesinin ve gerekli düzenlemelerinin yapılmasının zorunluluğunu ortaya koymuştur. Risk yönetimi yaklaşımlarında risk olaylarını sadece birer birer ele almayıp, birden fazla riskin birbirlerini nasıl etkileyeceğini irdeleyen risk senaryoları üretme ve bu senaryolara karşı yanıtları planlama açıklanmaktadır.

Bu çalışma risk yönetiminin Anonim Şirketlerde işlerliğini ve etkisinin değerlendirilmesi amacı ile hazırlanmıştır. Çalışma kapsamında Türkiye'de faaliyet gösteren bir Anonim Şirket'e risk yönetimi kavramının aşılanması ve böylece strateji belirleyip aksiyon alma süreçlerini ve riskleri göz önüne alarak yönetebilme yetileri kazandırılmaya çalışılmıştır.

GENERAL KNOWLEDGE

Name and Surname : Aytunç YILDIRIM

Field : Business Administration

Programme : Accounting Auditing

Supervisor : Professor Nuran CÖMERT

Key Words : Risk, Risk Management, Corporate Governance

ABSTRACT

Increasing level of competition, the density of products and services in incorporated business company increased likelihood of risks and influence of losses at organizations. Emerging of losses and scandals have revealed the necessity to develop risk management and perform the necessary arrangements. İn risk management, risk events aren't evaulated one at a time, It is evaulated how risk events affects each other, includes producing risk sceanarios and it also declarates the responds of these risk sceanarios.

This study has prepared with the aim of evaulating the operability and the effect of risk management in incorporated business company.Within the context of this study, It is aimed to get the concept of risk management thereby taking actions procedures in a Incorporated Business Company which is still operating company in Turkey.

İÇİNDEKİLER

Sayfa No.

BÖLÜM I

İÇ DENETİMİN TANIMI VE İŞLETMELERDE İÇ DENETİM FONKSİYONUNUN ROL VE SORUMLULUKLARI

BÖLÜM II

RİSK YÖNETİMİ VE İŞLETMELERDE RİSK YÖNETİMİNE İLİŞKİN MODELLER VE ULUSLARARASI STANDARLAR

BÖLÜM III

YENİ TÜRKTİCARET KANUNU KAPSAMINDA ANONİM ŞİRKETLERİN YAPISAL ÖZELLİKLERİ VE RİSK YÖNETİMİ'NİN ETKİLİLİĞİNİ DEĞERLENDİRME SÜRECİ

BÖLÜM IV

ANONİM ŞİRKETLERDE İÇ DENETİM BİRİMİNİN YAPILANDIRILMASI VE RİSK YÖNETİMİNDEKİ ROLÜ ÜZERİNE BİR UYGULAMA ÖRNEĞİ

TABLO LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

ABD	Amerika Birleşik Devletleri
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
COCO	Criteria of Control Objectives
COSO	The Committee on Sponsoring Organizations of the Treadway Commision
ERM	Enterprise Risk Management
IIA	Institute of Internal Auditors
İMKB	İstanbul Menkul Kıymetler Borsası
KRY	Kurumsal Risk Yönetimi
PCAOB	Public Company Accounting Oversight Board
SOX	Sarbanes–Oxley
SPK	Sermaye Piyasası Kurulu
TİDE	Türkiye İç Denetim Enstitüsü
TBMM	Türkiye Büyük Millet Meclisi
TTK	6102 Sayılı Türk Ticaret Kanunu
UİDS	Uluslararası İç Denetim Standartları
UMUÇ	Uluslararası Mesleki Uygulamalar Çerçevesi

GİRİŞ

1990'lı yılların ortalarında dış piyasalarda yaşanan ve dünyada şirketlerin iflas etmesiyle sonuçlanan gelişmeler piyasaların sorgulanmaya başlanmasına neden olmuştur. Şirketlerin başarısızlığı sonucu büyük kayıplar yaşayan hissedarlar, yatırımcılar ve toplum bu kayıplarının etkilerini azaltmak için yeni yöntemler arama yoluna girmiş, bu da hem kayıpların etkilerinin azaltılması hem de aynı tip kayıpların yeniden yaşanmaması için risk yönetiminin önemli bir kavram olarak görülmeye başlanmasına neden olmuştur.

Günümüzde kurumların içinde bulunduğu ortam çok daha karmaşıktır. Kurumların karşı karşıya olduğu küreselleşme, yeni kurumsal ortaklıklar, iş dünyasında hareketliliğin artması, sürekli değişim gibi durumlar; bu kurumların karşılaştıkları risklerin de çoğalmasına sebebiyet vermiştir. Risk yönetiminin artık, karşılaşılan tüm riskler için kullanılabilen bir araç olabilmesi için strateji, operasyon, itibar, yasal düzenlemeler ve bilgiyi de içeren çok geniş sorunları kapsar hale getirilmesi zorunluluk haline gelmiştir.

Yaşanan şirket skandalları, kötü yönetim, etkisiz kontroller ve denetim kalitesinin sorgulanması paralelinde bir tür erken uyarı görevi üstlenen iç denetimin önemi artmış 2000 yıllarının başında tanımı değiştirilerek mesleki uygulama standartları yeni bir çerçeveye kavuşturulmuştur. Bu kapsamda işletmenin faaliyetlerini geliştirmek ve onlara değer katmak amacıyla işletme içinde bağımsız ve tarafsız bir güvence ve danışmanlık hizmeti olarak tanımlanan iç denetime, işletmenin kontrolü, risk yönetimi ve yönetişim süreçlerinin etkililiğini değerlendirme görevi yüklenmiştir. Dünyadaki ve ülkemizdeki hileli finansal raporlama sorunları zaman içerisinde, risk yönetimi ve iç denetim kavramlarının yasa ve düzenlemelerde ele alınmasını gerektirmiştir.

Özellikle ard arda yaşanan küresel krizlerle alınan sınırsız riskler sorgulanır hale gelmiş ve çıkarılan derslerle bu risklerin yönetilmesine dair olumlu çalışmalar yapılmıştır. En önemli gelişme risk yönetiminin bir sonucu olarak işletmelerce yüklenilen riskli faaliyetlerin yönetiminin, denetlenmesini gerekli kılmasıdır. İşte bu noktada risk odaklı iç denetim gündeme gelmektedir.

Risk odaklı denetim ya da risk temelli denetim de esas olarak, risk yönetimi süreçlerinin çıktılarından yararlanır ve odak noktası olarak yüksek riskli alanları hedef

denetim alanı olarak seçer. Böylece denetimde etkililiğin artırılması, zaman ve maliyet tasarrufu sağlanmış olur.

Kurumların yönetimlerini güçlendirmeleri ve daha iyi yönetim modelleri oluşturmaları için yol göstermek amacıyla mesleki örgütlerce birçok ilke ve standart geliştirilmiş, rehberler basılmış, birçok kural oluşturulmuştur. Tüm bu rehberler, standartlar, kurallar birbirlerinden farklı olmalarına ve değişik kökenlere sahip olmalarına rağmen ortak olan yönleri etkili bir risk yönetim sisteminin geliştirilmesidir.

Değişen dış çevre koşulları karşısında işletmelerin rekabet yapabilmeleri ancak bu değişikliklere karşı etkili stratejiler geliştirmekle mümkün olabilmektedir. İşletmelerin stratejik olarak yönetilebilmesi, gerekli planlamaların yapılabilmesi, risk yönetimi ve risk odaklı iç denetim süreçlerinin karar alma süreçlerine eklenmesiyle mümkün olacaktır.

Bu tez çalışması kapsamında işletmenin risk yönetiminde iç denetimin üstlendiği rol ve sorumluluklar ele alınarak risk bileşenleri çerçevesinde Anonim Şirketlere Risk Yönetimi becerileri ortaya konulmaya çalışılmaktadır.

Bu amaçla ele aldığımız tezim giriş ve sonuç dışında dört bölümden oluşmaktadır.

Birinci Bölümünde, iç denetimin tanımı, iç denetimin unsurları ele alınarak açıklanmış, iç denetimin tarihsel gelişimi ve dünyada iç denetime bakış tarzı ele alınmıştır. Ayrıca iç denetçinin yönetişimle, iç kontrollerle ilgili sorumluluklarına da bu bölümde yer verilmiştir.

İkinci Bölümde, öncelikle kurumsal risk yönetim uygulama modellerine kronolojik olarak değinilmiş olup ardından uluslararası alanda en çok kabul gören COSO-KRY Modeli uygulama süreci ayrıntılarıyla ele alınmıştır.

Üçüncü Bölümde, Yeni Türk Ticaret Kanunundaki düzenlemeler çerçevesinde Anonim Şirketler' in yapısal özellikleri ve iç denetim faaliyetleri kapsamında risk yönetiminin etkililiği konularına değinilmiştir.

Dördüncü Bölümde ise, Anonim Şirketlerde iç denetim biriminin yapılandırılması ve risk yönetimindeki rolü üzerine bir uygulama örneğine yer

verilmiştir. Uygulama örneğinden elde edilen veriler önceki bölümlerde anlatılan COSO-KRY Modeline oturtularak örnek bir kurum analizi yapılmıştır.

Sonuç Bölümünde ise önceki bölümlerde açıklanan bilgiler ve uygulama çalışmasının sonuçları dikkate alınarak tezimizin bütünsel bir değerlendirmesi yapılmıştır.

BÖLÜM I

İÇ DENETİMİN TANIMI VE İŞLETMELERDE İÇ DENETİM FONKSİYONUNUN ROL VE SORUMLULUKLARI

1.1. İç Denetimin Tanımı

İç denetim faaliyetinin, Uluslararası İç Denetçiler Enstitüsü (Institute of internal Auditors, IIA) tarafından belirlenen günümüzdeki tanımı şu şekildedir;

"İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir. İç denetim kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistematik ve disiplinli bir yaklaşım getirerek kurum amaçlarının gerçekleştirilmesine yardımcı olur".[1]

Yukarıdaki tanım iç denetim faaliyetlerinin amacını, kapsamını, kurumsal yapı ve işleyişi içerisindeki önemini, ulaşmak istediği amaçları ve çalışma yöntemlerini güncel bir yaklaşımla açıklayan bir tanımdır. IIA tarafından geliştirilen "Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ)" ve bu çerçeve içerisinde yer alan "Uluslararası İç Denetim Standartları, (UİDS)" söz konusu tanımın unsurlarını açıklamakta ve bu unsurlara uygun olarak iç denetim faaliyetlerinin nasıl gerçekleştirileceğini düzenlemektedir. Standartları ve etik kuralları içeren çerçeve bir bütün halinde iç denetimin yukarıda yer verilen küresel tanımı ile birlikte günümüzdeki modern iç denetim uygulamalarının temelini oluşturmaktadır. İç denetim faaliyetinin yukarıdaki tanımına uluslararası alanda iç denetime ilişkin hemen hemen tüm düzenlemelerde rastlamak mümkündür.[2]

1.1.1. İç Denetim Tanımının Unsurları

İç denetimin ne olduğunu daha iyi kavramak için tanımında geçen unsurları aşağıdaki gibi sırasıyla açıklamakta fayda vardır.

Uluslararası iç denetim standartlarına göre bağımsızlık, tarafsızlığı ve tarafsızlık görüntüsünü bozabilecek şartların dışında olmayı gerektirmektedir. İç denetim faaliyeti,

---

[1] Institute of internal Auditors Inc. ,(Çevrimiçi: www.theiia.org, Erişim Tarihi: 18.01.2013)

[2] **‘’Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi”,** Türkiye İç Denetim Enstitüsü Yayınları, No:3, İstanbul, 2005. s.25.

denetlediği faaliyetlerden bağımsız; görev kapsamının belirlenmesi, görevlerin yerine getirilmesi ve sonuçlarının raporlanması konularında ise her türlü müdahaleden uzak olmalıdır[3].

İç denetim faaliyetinin bağımsızlığının sürdürülebilmesi için iç denetim yöneticisinin işlevsel olarak yönetim kuruluna, idari olarak da kurumun başkanına bağlı ve sorumlu olması gerekmektedir[4].Diğer bir ifadeyle iç denetim bir işletmede üst yönetim ve yönetim kurulu tarafından belirlenen politikalar ve prosedürler çerçevesinde işletme örgütünün ve fonksiyonlarının tamamlayıcı bir parçası olarak işletmedeki kontrollerin eksikliğini ölçmek ve değerlendirmek amacıyla yürütülen bir denetim faaliyetidir[5]

Tarafsızlık, iç denetçilerin görevlerini yaparken almaları ve sürdürmeleri gereken bağımsız bir zihinsel tavır olup, iç denetçilerin görevlerini, iş sonunda çıkan ürüne gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri şekilde yapmalarını ve yürütmelerini gerektirmektedir.[6]

Uluslararası İç Denetçiler Enstitüsü iç denetimi bir danışmanlık ve güvence faaliyeti olarak tanımlamıştır. Enstitü danışmanlık faaliyeti ile burada herhangi bir idari sorumluluk üstlenmeden, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı denetlenen ile birlikte kararlaştırılan faaliyetleri ve buna bağlı diğer hizmetleri kastetmektedir.[7]

Uluslararası İç Denetçiler Enstitüsü tanımında iç denetimi, amacı organizasyonun faaliyetlerini geliştirmek ve onlara değer katmak olan bir faaliyet olarak ifade etmiştir. Enstitü'ye göre iç denetim, güvence ve danışmanlık hizmetleri yoluyla, kurumun amaçlarını gerçekleştirme fırsatlarını geliştirerek, faaliyetleri geliştirme imkanlarını belirleyerek ve/veya riske maruz kalmasını azaltarak faaliyetlere değer katabilir.[8]

---

[3] Türkiye İç Denetim Enstitüsü Yayınları, a.g.e. s.25.
[4] Türkiye İç Denetim Enstitüsü Yayınları, a.g.e. s.25.
[5] Nuran Cömert , **''Sermaye Piyasası Aracı Kurumlarında Etkili Bir İç Kontrol Sistemi ve Denetim Fonksiyonu''**, Lebib Yalkın Matbaası, İstanbul 2002, s.56
[6] Türkiye İç Denetim Enstitüsü Yayınları, a.g.e. s.25.
[7] Türkiye İç Denetim Enstitüsü Yayınları, a.g.e. s.27.
[8] Türkiye İç Denetim Enstitüsü Yayınları, a.g.e. s.27.

Bir işletmede iç denetçiler tarafından genel olarak işletme yöneticilerine sorumluluklarını etkili ve verimli bir şekilde yerine getirmelerine yardımcı olmak amacıyla yürütülen bir denetim faaliyetidir.[9]

İç denetimin, organizasyonun faaliyetlerini geliştirmesi ve onlara değer katabilmesi için öncelikle o faaliyetin sonuçlarını kullananları, yani müşterilerini tespit etmesi gerekmektedir. Bu bağlamda faaliyet sonuçlarının pek çok kullanıcısının olması, iç denetim faaliyetinin bir o kadar müşterisinin olması anlamına gelmektedir. Bu müşteriler arasında, denetlenen birim, denetim komitesi, üst yönetim, finansal yönetim, kanun koyucular, bağımsız dış denetçiler, alıcılar ve tedarikçiler sayılabilir. Sadece iç denetim faaliyetinin müşterileri değil, aynı zamanda faaliyetlere ne gibi bir değer katılacağı da organizasyonun yapısı ve kurum kültürüne göre çeşitlilik gösterebilir.

Örneğin işletme müdürü, iç denetimin faaliyetlerin etkililiğini ve verimliliğini arttırması ile ilgilenirken; bağımsız dış denetim iç denetime, etkili çalıştığı durumda, finansal tablolar üzerindeki çalışmalarının kapsamını azaltacak ek bir kontrol olarak bakmaktadır. Alıcı ve satıcılar ise iç denetimi organizasyon içindeki bilgi akışının güvenilirliği ve gizliliğine ilişkin güvence sağlayan bir faaliyet olarak görmektedir.[10] Önemli olan iç denetim müşterilerin iç denetim faaliyetlerini maliyet yaratan ve süreçleri yavaşlatan bir unsur olarak değil, katma değer sağlayan bir fonksiyon olarak görmelerini sağlamaktır. Bunu sağlayabilmek için ise iç denetçilerin iç kontrol ve risk yönetimi konularındaki değerlendirmeleri, çeşitli risklere karşı tasarlanıp, uygulamaya konulan iç kontrol ve risk yönetimi sistemlerinin maliyeti ve bu sistemlerin mevcut olmaması halindeki kayıpları ortaya koymalı ve bu iki durumun karşılaştırılmasını da içermelidir.[11]

İç denetimin işletmeye sağladığı değerin arttırılmasında iç denetçilere büyük görevler düşmektedir. İç denetçiler, meslek ile ilgili uluslararası standartların, güncel kavram ve uygulamaların farkında olmalı, literatürü yakından takip etmeli ve mesleki gelişimleri yönünde çaba sarf etmelidirler. Sahip oldukları risk ve iç kontrol deneyimi ile bu konudaki bilgi ve birikimlerini kurum yararına kullanmalı ve kuruma

[9] Erdal Polat, **Denetimde Beşeri Unsurun Rolü ve Önemi**, Uzman Gözüyle Bankacılık Dergisi, Sayı23,Eylül 1998, s.6.
[10] Urton Anderson, **"Assurance and Consulting Services",** The Institute of Internal Auditors Research Foundation, 2002, www.theiia.org/iia/download.cfm?file=1777,(14.02.2013) s.5.
[11] N. Burak Ünlü, "Kurumlarda İç Denetimin Değerinin Arttırılması**", Türkiye İç Denetim Enstitüsü İç Denetim Dergisi**, Sayı 9, Sonbahar 2004, s.24.

alışılagelmiş iç denetim yaklaşımının dışında da fayda sağlayabileceklerini ortaya koymalıdırlar. Özellikle risk odaklı denetim gibi yeni ve daha fazla katma değer sağlayan yaklaşımlarda denetçinin bilgi ve tecrübesi denetim sürecinin her aşamasında çok büyük önem taşımaktadır.[12]

1.2. İç Denetimin Tarihsel Gelişimi

İç denetim tarihini muhasebenin ve bağımsız denetimin tarihiyle aynı paralelde açıklayan görüşler bir yana modern iç denetimin tarihi ABD de 1941 yılında bugünkü Uluslararası İç Denetçiler Enstitüsünün temelini oluşturan İç Denetim Enstitüsünün kurulmasıyla başladığı kabul gören bir yaklaşımdır.

Tarihsel olarak dünyada iki ana hukuksal sistem bulunmaktadır. Asya ülkelerinin tarihsel geçmişinden ve binlerce yıl öncesine dayanan uygarlığından gelen kendilerine özgü devlet ve toplum gelenekleri bir kenarda tutulursa Avrupa ülkelerinde ve Avrupa uygarlığı kaynaklı toplumlarda (ABD, Kanada, Avustralya vb.) iki temel hukuk sistemi Ön plana çıkmaktadır. Bunlardan birincisi köklerini Roma Hukukundan alan "Civil Law" (Medeni Hukuk), diğeri ise Anglosaxon kaynaklı "Common Law" (İçtihat Hukukudur). [13]

Prof. Dr Necdet Şensoy, her iki gelenek arasında hukuk sistemleri, şirketlerin sahip yapısı ve mesleki örgütlenmeler de dahil olmak üzere bazı farklılıklar olduğunu, Kıta Avrupası Ülkelerinde Roma Hukuku ile detaylı kodifikasyonun söz konusu olduğunu buna karşın anglosaxon sistemde örf ve adet hukukunun (Common Law)' ın söz konusu olduğunu, statüler yerine mahkeme kararlarının ve kıyasın uygulandığını, dünya çapında piyasalaşma ve küreselleşme yaygınlaştıkça işletme yönetimi, finansal raporlama ve denetimde anglosaxon geleneğin küresel kabul gördüğünü ifade etmektedir.[14]

---

[12] John Fraser , Hugh Lindsay**," Yönetim Kurullarının İç Denetim Hakkında Sorması Gereken 20 Soru".**Mehtap Doğan ve Diğerleri (çev.), *IAA Bullettin* ,(Çevrimiçi:http://tide.org.tr/tideweb/resimler/upload/Documents/Y%C3%96NET%C4%B0M%20KURULLARININ%20%C4%B0%C3%87%20DENET%C4%B0M%20HAKKINDA%20SORMASI%20GEREKEN%2020%20SORU%20(IIA).DOC, Erişim Tarihi: 12.01.2012),s.2.

[13] Bu konuda ayrıntılı bilgi için bakınız. Çetin ÖZBEK, ‘**’İç Denetim’’** TİDE Yayınları ,Yayın No:3 s.4-20 , İstanbul ,Ekim,2012

[14] Necdet Şensoy **“Kurumsal Yönetim Bağlamında Kurumlarda Finansal Raporlama, Kontrol ve Denetim“** Çukurova Üniversitesi, Sunum:25 Nisan 2011

Modern iç denetim'in "kurucusu" olarak bilinen Lawrence B. Sawyer, iç denetim mesleğinin tarihini ağırlıklı olarak ABD perspektifi açısından incelemekle birlikte; günümüzdeki iç denetim uygulamalarının gelişimi ve şekillenmesinde ABD'nin tecrübelerinin çok büyük etkiye sahip olması nedeniyle bu ülkeye özgü gelişmelere değinmek günümüz iç denetim metodolojisinin temelinde yatan düşünceleri anlayabilmek açısından önem taşımaktadır. Sawyer, ABD de iç denetimin gelişimi konusunda şu bilgileri vermektedir;[15]

"18 ve 19. yüzyıl boyunca kurumların, finansal kayıtlarını kontrol etmeleri için muhasebeci istihdam etmeleri, denetim mesleğini "işitmenin" ötesinde yazılı kayıtların dikkatli gözden geçirilmesi ve muhasebe girişlerinin evrak üzerinden delillerle karşılaştırılması şekline dönüştürmüştür. Koloniyal dönemde İngiliz müteşebbislerinin o tarihteki Amerika 'ya yaptıkları yatırımların bağımsız bir şekilde denetlenmesini istemeleri sonucunda İngiliz denetçilerin denetim metot ve prosedürleri ABD'ye getirilmiştir. O tarihteki Britanya Şirketler Kanunu'nun yatırımcıları daha fazla hesap verebilirlikle sorumlu tutması denetimde muhasebe hesaplarının daha analitik bir yaklaşımla denetlenmesinin yanı sıra finansal tablolar denetimine ağırlık verilmesine yol açmıştır. ABD'de demiryolu şirketleri yöneticilerinin ülke boyunca yayılmış istasyonlarındaki personelinin gelirleri doğru kaydettiklerinden emin olmak istemeleri ve dış denetimin sisteminin bu konularda yetersiz kalması ilk uzak mesafelerdeki iç denetim programlarının uygulanmasını sağlamıştır. Tarihsel süreç içerisinde iş ve kamu kesimi operasyonlarındaki karmaşıklığın artması iç denetimin gelişmesinde sürekliliğe yol açmıştır.''

Muhasebe ve bağımsız denetim uygulamalarındaki tarihsel gelişime paralel olarak iç denetim faaliyetleri özellikle II. Dünya Savaşına kadar olan dönemde bağımsız denetim faaliyetlerinin kurum içerisindeki bir uzantısı olarak muhasebe sisteminin ve finansal raporların denetimi ile sınırlı bir profil çizmiştir.

İç denetimin devam eden gelişmesi, işlerin ve yönetim faaliyetlerinin zaman içerisinde daha karmaşık hale gelmesi nedeni ile olmuştur. Yönetimin, işletme faaliyetlerini

[15]Lawrence Sawyer Mortimer D.Dittenhofer, James H.Scheiner,**''Sawyer's Internal Auditing'',** 2003, 5th Edition, s. 3'den aktaran, Özbek, **İç Denetim**, s.6.

izlemekte yetersiz kalması ile birlikte iç denetim önemli bir fonksiyon haline gelmeye başlamıştır.[16]

Çetin Özbek 'in kitabında atıfta bulunduğu kaynaklara göre, modern iç denetim faaliyetlerinin gelişimi II. Dünya savaşından sonra gerçekleşmiştir. Büyük oranda günümüzdeki iç denetim uygulamalarının kapsam ve metodolojisinin oluşmasında etkili olan hususları iki grup halinde incelemek mümkündür. İlk grup altında dünya ekonomilerinde yaşanan değişimler, ekonomi ve ticaret kurallarındaki artan düzenlemeler, globalleşme, bilişim teknolojilerindeki gelişmeler, kurumsal yönetim, risk yönetimi ve iç kontrol kavramı gibi dışsal faktörlerdeki gelişmeler ve bu gelişmelerin iç denetim mesleğine olan etkileri, ikinci ve diğer grupta ise 1941 yılında ABD'de iç Denetim Enstitüsü (Institute of Internal Auditors, IIA)'nün kuruluşu ve iç denetim mesleğiyle ilgili yaptığı profesyonel çalışmalar sayılabilir.[17]

İç denetimin gelişimini etkileyen dışsal dolaylı gelişim unsurları şu şekilde sıralanabilir.[18]

- Küreselleşme,
- Bilişim teknolojilerindeki gelişim,
- Kurum operasyonlarının karmaşıklaşması ve uzmanlaşma,
- Kurumsal yönetim kavramındaki gelişimler,
- Risk yönetiminin gelişimi,
- İç kontrol kavramının gelişmesi.

2004 yılı Ocak ayından itibaren geçerli olmak üzere, IIA'nın İç Denetim Standartları Kurulu(Internal Auditing Standards Board) tarafından önemli ölçüde tadil edilen standartlar, günümüzün risk yönetimi ve kurumsal yönetim gerekliliklerini karşılayacak şekilde ve danışmanlık faaliyetlerine ve görev sonuçlarının kurum dışı taraflara sunulması konularına temas edecek şekilde güncellenmiştir.

ABD'deki gelişmeler hiç şüphesiz bu ülkenin ekonomik gücü sebebiyle değişen ilkeleri de etkilemiştir.1982 yılında (ECIIA) Avrupa İç Denetim Enstitüleri Konfederasyonunun kurulması ile mesleğine Avrupa Birliği'nde bir statü

[16] M.Ali Madendere, **''Kurumsal Risk Yönetiminde İç Denetimin Rolü,''** Yayımlanmamış TİDE Döküman,, Ekim 2005, s.9.
[17] Çetin Özbek, **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol,** TİDE Yayınları Yayın No:3 İstanbul, Ekim 2012, s 8.
[18] KAYA, Ertuğrul Bertan, **''İç Denetçi Eğitim Dokümanları,''** İstanbul, 2008, s.21.

kazandırılmıştır. Ülkemizde bu paralelde 1995 yılında kurulan (TİDE) Türkiye İç Denetim Enstitüsü ile ulusal sivil bir mesleki örgütlenme gerçekleşmiştir. TİDE ile başlayan meslektaşların örgütlenmesi, IIA nezdinde kabul görmüş ve Türkiye'de iç denetimin uluslararası standartlarda uygulanması, meslek mensuplarının uluslararası sertifikasyonu için imkan sağlamıştır.[19]

IIA' ın Türkiye Chapter 'ı olarak kabul görmesi yanında TİDE, 1997 yılında ECIIA (Avrupa İç Denetim Enstitüleri Konfederasyonu, European Confederation of Institues of Internal Auditing) üyeliğine de kabul edilerek, Türkiye'nin iç denetim mesleği açısından uluslararası alanda temsil edilmesini sağlamıştır. Ülkemizde iç denetim uygulamalarını etkileyen diğer gelişmelere baktığımızda; Avrupa Birliği müzakere süreci, Sermaye Piyasası Kurumu'nun düzenlemeleri, yeni bankacılık kanunu ve 6102sayılı Yeni Türk Ticaret Kanunu, 5018 sayılı Kamu Mali Yönetim ve Kontrol Kanunu dünyadaki gelişmelerden etkilenen düzenlemeler olarak sıralanabilir. Diğer taraftan SPK tarafından yayınlanan kurumsal yönetim ilkeleri ve uyum süreci, uluslararası yatırımlar için ilgi odağı haline gelmiş ülkemizde uluslararası iş birliği fırsatları yaratmakta ve Basel II düzenlemeleri ile kurumsal yönetim ilkelerinin benimsenmesiyle iç kontrol ve iç denetim biraz daha fazla ön plana çıkmaktadır.[20]

1.3. İç Denetçinin Sorumlulukları

Daha önce açıkladığımız iç denetimin tanımında da belirttiğimiz üzere iç denetim işletmenin yönetişim, iç kontroller ve risk yönetim süreçlerinin etkililiğini değerlendirme sorumluluğunu üstlenmiştir. Bu üç temel sorumluluk alanı kapsamında iç denetim sistemli bir yaklaşımla çalışarak güvence ve danışmanlık hizmetlerini yerine getirir ve organizasyonun amaçlarının başarılmasına yardımcı olur. Burada amaç ile kastedilen olgu başarılılık, güvenilir işletme olma yasaya ve düzenlemelere uygun faaliyetlerde bulunmaktır.[21]

---

[19] UZUN, A. Kamil., **Aile İşletmelerinde Kurumsal Yönetim ve İç denetimin Rolü,** Deloitte Kurumsal Yönetim Makaleleri, http://www.denetimnet.net/Pages.aspx?pgID=388, (Erisim:15.08.2012) s.1.

[20] UZUN, A. Kamil., **İç Denetim İle İlgili Düzenleme ve Uygulama Sürecinde Basarı İçin Yol Haritası,** (Çevrimiçi:http://www.denetimnet.net/Pages.aspx?pgID=389, Erisim: 17.08.2012) s.1.

[21] Nuran Cömert, **''Denetim,İç Kontrol , İç Denetim Konusunda Dünyada veÜlkemizdeki Gelişmeler Konusunda Bir Son Durum Değerlendirmesi,''** III. Türkiye Sektörel Muhasebe Uygulamaları Sempozyumu Panel Notları , Kayseri, Hilton Oteli, (19.01.2013)

1.3.1. İç Denetçinin Yönetişim İle İlgili Sorumlulukları

Günümüzde artık yaygın bir şekilde yönetişim, ülkelerin kaynaklarının ekonomik ve toplumsal gelişme için nasıl kullanılacağını belirleyen gelenekler ve kurumsal yapılar olarak görülmeye başlanmıştır. Kararların nasıl alındığı, gücün nasıl kullanıldığı ve ülke insanlarının bu sürece nasıl katıldığı konusundaki uygulamalar ise yönetişimin kalitesini belirlemektedir. Bu süreçte yönetişimin amacı, hem toplumsal sorunlarla hem de çağdaş toplumların karmaşıklığını, dinamikliğini ve çeşitliliğini yaratan olgularla baş edebilmek olmaktadır. Karmaşıklık, toplumsal dinamikler ve çeşitlilik, yeni oluşan toplumsal alt sistemler nedeniyle devletlerin içsel egemenliğinin azalmasına yol açabilmektedir. Bundan dolayı çağdaş yönetimin amacının, öncelikle toplumsal aktörleri harekete geçirmek ve onları eşgüdümlemek olması gerektiği söylenmektedir. Yönetişim, toplumsal çıkarları dengelemekte ve toplumsal aktörlerin ve dizgelerin kendilerine çekidüzen vermelerini sağlayacak biçimde olanakları ve sınırlılıkları ortaya çıkarmaktadır.[22]

İç denetim faaliyeti, aşağıdaki amaçların gerçekleştirilmesi amacıyla yönetişim sürecini değerlendirmek ve iyileştirilmesi için gerekli tavsiyelerde bulunmak zorundadır. Bu tavsiyeler;[23]

• Kurum içinde gerekli etik ve diğer değerlerin geliştirilmesi,

• Etkili bir kurumsal performans yönetiminin ve hesap verebilirliğin temini,

• Risk ve kontrol bilgilerinin kurumun gerekli alanlarına iletilmesi,

• Yönetim kurulunun, denetim kurulunun, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin iletimini sağlamaktır.

Uluslararası İç Denetim Mesleki Uygulama Standartları, yönetişimi; "Kurumun amaçlarının başarılmasına yönelik olarak Yönetim Kurulu tarafından faaliyetlerin bildirilmesi, yönlendirilmesi, yönetilmesi ve izlenmesi için uygulanan yapı ve süreçlerin bir birleşimi" olarak tanımlamaktadır.

---

[22] Seriye SEZEN, ,'' **Kamu Yönetimi Sözlüğü,''** TODAİE Yayınları, Ankara. 1998,s.14
[23] Uygulama Önerisi 2110-2, Nisan 2010

Yönetişim bir takım farklı ve ayrı ayrı süreç ve yapılardan oluşmaz. Yönetişim, risk yönetimi ve iç kontrol arasında oldukça fazla ilişki vardır.

Etkili yönetişim iç kontrollere ve bu kontrollerin etkililiği konusunda Yönetim Kurulu'yla olan iletişime dayanır.

Bir kurumun etkili yönetişimin ilkelerini nasıl tasarlayacağı ve uygulayacağı o kuruluşun büyüklüğüne, karmaşıklığına, yaşam süresindeki olgunluğuna, paydaşlarının yapısına, yasal ve kültürel gereksinimlerine vs. bağlı olarak da değişiklik gösterir. Yönetişimin tasarım ve yapısındaki değişkenliklerin bir sonucu olarak, İç Denetim Yöneticisi'nin, denetim amaçları açısından yönetişimin en uygun şekilde nasıl tanımlanacağına karar verebilmek için, Yönetim Kurulu ve üst yönetim ekibiyle birlikte çalışması gereklidir.[24]

İç denetim kurumun yönetişim çerçevesinin ayrılmaz bir parçasıdır. İç denetçilerin kurum içindeki kendilerine özgü konumları yönetişim yapısını, tasarımını ve işleyişinin etkililiğini bağımsız olarak gözlemlemelerine ve biçimsel(resmi) olarak değerlendirmelerine imkân tanır. Yönetişim, risk yönetimi ve iç kontrol arasındaki ilişkinin göz önünde bulundurulması gereklidir. [25]

IIA 'ın uygulama önerilerine göre; İç Denetim Yöneticisi' nin yönetişim süreçlerinin değerlendirilmesini planlarken aşağıdaki ilişkileri göz önünde bulundurması gereklidir: [26]

1. *Bir denetimin, örgütsel stratejilerin, amaçların ve faaliyetlerin etkililiğini ve verimliliği, finansal raporlama ve ilgili yasalara ve diğer düzenlemelere uygunluk amaçlarının başarılmasını olumsuz etkileyebilecek olayları önlemek veya ortaya çıkarmak için yönetişim süreçleri içinde tasarlanan kontrollere yönelmesi gereklidir.*

2. *Yönetişim süreçlerindeki kontroller çoğu kez kurumun karşılaştığı çok yönlü risklerin yönetilmesinde önemlidir. Örneğin uygunluk riskleri, hile riskleri vb.nin yönetilmesi için davranış kuralları çevresindeki kontrollere güvenilebilir. Yönetişim süreçlerinin denetim kapsamı*

[24] Patchin Curtis, **''Coso, Rsk Assessment Practice ,''** October 2012 s.5.
[25] Fraser, Lindsay ,s.6.
[26] Uygulama Önerisi 2110-3

belirlenirken risk ve kontrolün birlikte etkisinin göz önünde bulundurulması gereklidir.

3. *Eğer diğer denetimler yönetişim süreçlerindeki kontrolleri değerlendiriyorsa denetçinin o denetimlerin sonuçlarına güvenmeyi düşünmesi gereklidir.*

1.3.2. İç Denetçinin İç Kontroller İle İlgili Sorumlulukları

Günümüzde iç kontrol bir işletmenin üst yönetimi ve diğer personeli tarafından etkilenen, işletmenin faaliyetlerinin etkililiği, finansal raporlanmasının güvenilirliği yasalara ve düzenlemelere uygunluk amaçlarını başarmak üzere tasarlanmış bir süreç olarak tanımlanmaktadır.[27]

İç denetim faaliyeti, aşağıdaki amaçların gerçekleştirilmesi amacıyla yönetişim sürecinin iyileştirilmesi için gerekli tavsiyelerde bulunmalı ve tavsiyeleri değerlendirmelidir:[28]

- *Kurum içinde gerekli etik ve diğer değerlerin geliştirilmesi,*
- *Etkili bir kurumsal performans yönetimi ve hesap verebilirlik,*
- *Risk ve kontrol bilgilerinin kurumun gerekli alanlarına etkili bir şekilde iletilmesi,*
- *Yönetim kurulunun, denetim kurulunun, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin etkili bir şekilde iletimini sağlamak.*

Riski yönetmek ve belirlenmiş hedeflere ulaşma olasılığını artırmak amacıyla yönetim, Yönetim Kurulu ve diğer taraflarca alınan herhangi bir tutum olarak tanımlanan kontrolün tanımında da belirtildiği üzere kontrol ve risk birbiriyle ilişkilidir.

Bu sebeple işletme içerisinde bir takip sistemi oluşturulması, işletme ile koordinasyonun sağlıklı bir şekilde kurulması ve devamlılığının sağlanması gerekmektedir.[29]

---

[27] (Çevrimiçi: www.coso.org , Erişim: 02.02.2013)
[28] Uygulama Önerisi 2130
[29] Özgür Çatıkkaş, Gürdoğan Yurtsever, **''Türk Bankacılık Sektöründe Denetim Komitesi Uygulaması''**, İç Denetim Dergisi, Yaz 2007, s.38.

1.3.3. İç Denetçinin Risk Yönetimi İle İlgili Sorumlulukları

Uluslararası İç Denetim Standardı iç denetim faaliyetinin, işletmenin risk yönetimi süreçlerinin etkililiğini değerlendirmesini ve iyileştirilmesine katkıda bulunmasını öngörmektedir. Buna göre iç denetçi mesleki yargısını kullanarak aşağıdaki konularda değerlendirmeler yapmalıdır.

Risk değerlendirmesinin sonuçlarına bağlı olarak, iç denetim faaliyeti, kurumun yönetimini, faaliyetlerini ve bilgi sistemlerini kapsayan kontrollerin yeterliliğini ve etkinliğini değerlendirmelidir.

Bu değerlendirme:[30]

- *mali ve operasyonel bilgilerin güvenilirliğini,*
- *faaliyetlerin etkinlik ve verimliliğini,*
- *varlıkların korunmasını,*
- *kanunlara, düzenlemelere ve sözleşmelere uyum konularını kapsamalıdır.*
- *İç denetçiler, faaliyet ve programların hedef ve amaçlarının kapsamını ve bunların kurumun hedef ve amaçlarına uyumunun derecesini anlayıp değerlendirmelidir.*
- *Danışmanlık görevleri sırasında, iç denetçiler, görevin amaçlarıyla uyumlu bir şekilde kontrolleri ele almalı ve herhangi bir kontrol zafiyetine karsı uyanık olmalıdır.*
- *İç denetçiler, danışmanlık görevlerinden elde ettikleri kontrol bilgilerini, kurumun maruz kaldığı önemli riskleri belirleme ve değerlendirme sürecinde kullanmalıdır.*

İç denetçi organizasyonda en üst birime, varsa denetim komitesi, yoksa yönetim kurulu veya genel müdüre, bağlı olarak faaliyette bulunmalı ve tarafsızlığına gölge düşürmemek için uzun süre aynı işletmede iç denetçi olarak çalışmamalıdır.[31]

[30] Uygulama Önerisi 2120-1

[31] Jale Sağlar, **"Bağımsız ve İç Denetimde Kalite Kontrolü: Bağımsız Denetim Firmaları ile Büyük Sanayi İşletmeleri Üzerinde İki Farklı Saha Araştırması",** Doktora Tezi, Adana, 2003, s.115.

1.3.4. Uluslararası İç Denetim Standartları Kapsamında Risk Yönetimi

İç Denetim'in daha önce verdiğimiz tanımdan hatırlayacağımız üzere kurumun risk yönetimi süreçlerinin etkililiğini değerlendirmek denetçinin asli görevlerinden biridir. Bu husus 2120 nolu Uluslararası İç Denetim Standartlarında şu şekilde düzenlenmiştir.

İç denetim faaliyeti; risk yönetimi süreçlerinin etkililiğini değerlendirmek ve iyileştirilmesine katkıda bulunmak zorundadır.

Bu standarttan; Risk yönetimi süreçlerinin etkili olduğuna karar vermek, iç denetçinin aşağıdaki konulardaki değerlendirmelerinin doğurduğu bir yargı olduğu anlaşılmaktadır. Ayrıca ilgili standarttan aşağıdaki çıkarımları yapmakta mümkündür.

- Kurumsal amaçlar, kurumun misyonunu destekliyor ve onunla aynı paraleldeyse,
- Önemli riskler belirlenmiş ve değerlendirilmişse,
- Riskleri kurumun risk iştahı ile aynı paralele getiren uygun risk cevapları seçildiyse,
- Personelin, yönetimin ve yönetim kurulunun sorumluluklarını yerine getirmesine yardımcı olan ilgili risk bilgisi elde edilip zamanında kurum genelinde yayımlandıysa,

İç denetim faaliyeti bu değerlendirmeleri destekleyecek bilgileri çok sayıda görev sırasında toplayabilir. Bu görevlerin sonuçları, bir bütün halinde değerlendirildiğinde kurumun risk yönetimi süreçleri ve etkililiği konusunda bir fikir verir. Risk yönetimi süreçleri, devam eden yönetim faaliyetleri veya ayrı değerlendirmeler veya bunların her ikisi ile izlenir.

Konuyla ilgili güvence ve danışmanlık standartları yapılan çalışmanın niteliğinin güvence ve danışmanlık faaliyeti olması hallerinde uyulması gereken standartları açıklamaktadır. 2120.A.1 nolu güvence Standardına göre;

İç denetim faaliyeti, aşağıdakileri dikkate alarak, kurumun yönetişim süreçlerinin, faaliyetlerinin ve bilgi sistemlerinin maruz kaldığı riskleri değerlendirmek zorundadır:

- *Mali ve operasyonel bilgilerin güvenilirliği ve doğruluğu,*
- *Faaliyetlerin ve programların etkililik ve verimliliği,*
- *Varlıkların korunması,*
- *Kanun, düzenleme, politika, prosedürler ve sözleşmelere uyum.*

2120 A.2 nolu güvence standardına göre ise; İç denetim faaliyeti, suistimalin gerçekleşme ihtimalini ve kurumun suistimal riskini nasıl yönettiğini değerlendirmek zorundadır.

Söz konusu standartta danışmanlık hizmetleri kapsamında yer alan esaslar ise şöyledir:

- *İç denetçiler, danışmanlık görevleri sırasında, görevin amaçlarıyla uyumlu şekilde riski ele almak ve diğer önemli risklere karşı uyanık olmak zorundadır. İç denetçiler, danışmanlık görevlerinden elde ettikleri risk bilgilerini, kurumun risk yönetim süreçlerini değerlendirmede kullanmak zorundadır.*
- *İç denetçiler, risk yönetim süreçlerini kurmada veya geliştirmede yönetime yardım ederken, "riskleri gerçekte yönetmek suretiyle yönetim sorumluluğu almaktan" kaçınmak zorundadırlar.*

Önceki paragrafta açıkladığımız Uluslararası İç denetim Standartları ‘nın kapsamından anlaşılacağı gibi iç denetçinin KRY sürecindeki sorumluluğunu ikiye ayırabiliriz.[32]

1. Güvence hizmetleri kapsamında sorumluluğu
2. Danışmanlık hizmetleri kapsamında sorumluluğu ‘dur.

[32] Gerrit Sarens, ve Ignace De Beelde, “Contemporary internal auditing practices: New Roles and Influacing Variables. Evidence from exented case studies”, **Working Paper**, (October 2004)S.273, s.3

1.3.5. KRY Süreçlerinin Etkililiğini Değerlendirmede İç Denetçinin Sorumluluğu

Konuyla ilgili 2120-1 no'lu uygulama önerisi, iç denetim faaliyetinin kurumun risk yönetimi uygulamalarındaki yerini, 2120-2 no'lu uygulama önerisi de iç denetim faaliyetinin kendi faaliyetlerine yönelik risklerin nasıl yönetilmesi gerektiğini açıklamaktadır.

Konumuzla ilgili olan 2120-1 Risk Yönetimi Süreçlerinin Yeterliliğinin Değerlendirilmesi başlıklı uygulama önerisi, risk yönetimi süreçlerinin değerlendirilmesinde iç denetimin rolüne ilişkin şu önerilerde bulunmaktadır;[33]

1. *Risk yönetimi, kurum yönetiminin, yönetim kurulunun temel sorumluluklarından biridir. Kurumun hedeflerine ulaşabilmek için, yönetimin, kurum içinde sağlam risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını tespit etmek konusunda gözetim görevini üstlenmiştir. Bu görev kapsamında yönetim kurulu, iç denetim faaliyetini, yönetimin uyguladığı risk süreçlerinin yeterliliği ve etkililiğini incelemesi, değerlendirmesi, rapor etmesi ve bu konuda iyileştirici önlemler önermesi için yönlendirerek kendilerine destek olmasını sağlayabilir.*

2. *Kurumun risk yönetimi ve kontrol süreçlerinden üst yönetim, ve yönetim kurulu sorumludur. Ancak, danışmanlık rolünü Üstlenen İç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi ile risk yönetimi yöntemlerinin uygulanması, bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında kuruma yardımcı olabilirler.*

3. *Kurumun resmî risk yönetim süreçlerine sahip olmadığı durumlarda, iç denetim yöneticisi; üst yönetim ve yönetim kurulu ile kurum içinde riski anlamalarına, yönetmelerine ve izlemelerine yönelik yükümlülükleri hakkında görüşür ve üst yönetimin ve yönetim kurulunun, resmî olmasa bile, kendilerini tatmin edecek, kurum içinde anahtar risklerin görülebildiği uygun bir seviyede bir bilgi sağlayan ve risklerin nasıl*

[33] Uygulama Önerisi 2120-1

yönetilebileceğini ve izlenebileceğini belirten süreçlerin varlığının gerekli olduğu konusunu tartışır.

4. *İç Denetim Yöneticisi, kurumun risk yönetimi sürecinde, üst yönetim ve yönetim kurulunun iç denetim faaliyetinden beklentilerini öğrenmeli ve kavramalıdır. Bu bilgiler, iç denetim yönetmeliğine ve yönetim kurulunun yönetmeliklerine de yazılmalıdır. İç denetimin sorumluluklarının, kurumun*

• hiç rolü olmamaktan,

• iç denetim planının bir parçası olarak risk yönetimi sürecini denetlemeye,

• gözetim komitelerine, izleme faaliyetlerine ve durum raporlama

çalışmalarına katılmak gibi, risk yönetim sürecinde faal ve kesintisiz destek ve katılıma,

• risk yönetim sürecinin yönetimi ve koordinasyonuna kadar uzanan bir aralıkta olabilir.

Yukarıda açıkladığımız uygulama önerisinden anlaşılacağı üzere risk yönetiminin nihai sorumluluğunu yönetim kurulu ve üst yönetime verilmiştir. Ancak yönetim kurulu ve üst yönetim bu amaçla iç denetim faaliyetini etkili bir şekilde kullanabilmelidir.

İç denetim biriminin kurumun risk yönetimi sürecindeki katkısı kurum içerisindeki risk yönetimin gelişmişliği ile ters orantılıdır. Eğer kurum içerisinde güçlü bir risk kültürü varsa, gayet başarılı dizayn edilmiş ve iyi işleyen bir risk yönetimi mevcutsa, birim yöneticileri kendi sorumluluk alanlarındaki risklerini yönetme de başarılı ise iç denetim biriminin rolü, bu süreçlerinin etkinliğinin değerlendirilmesi ve üst düzey yöneticiler ve yönetim kuruluna raporlanması ile sınırlı olacaktır. Ancak bu konulardaki yetersizlikler arttıkça iç denetim biriminin risk yönetim sürecine daha fazla dahil olması gerekecektir. Bu durumda iç denetim faaliyetleri, kendi temel faaliyetlerine odaklanma ile danışmanlık yoluyla risk yönetimi süreçlerine dahil olma arasında bir yelpazede gidip gelecektir. IIA İngiltere ve İrlanda Enstitüsü tarafından yapılan bir değerlendirme de iç denetçilerin kurumun risk yönetimi faaliyet ve süreçlerine yönelik

olarak güvence ve danışmanlık faaliyetleri kapsamında üstlenebileceği roller ile hiç üstlenmemesi gereken roller şu şekilde sıralanmaktadır:[34]

Güvence fonksiyonları kapsamında üstlenilebilecek roller;

- *Risk yönetimi süreçleri hakkında güvence verilmesi,*
- *Risklerin doğru bir şekilde değerlendirildiğine dair güvence verilmesi,*
- *Risk yönetimi sürecinin değerlendirilmesi,*
- *Önemli risklerin raporlarıma sürecinin değerlendirilmesi,*
- *Önemli risklerin yönetilmesinin gözden geçirilmesi.*

Danışmanlık faaliyetleri kapsamında üstlenilebilecek roller;

- *Risklerin tanımlanması ve değerlendirilmesinin kolaylaştırılması,*
- *Risklerin giderilmesinde yönetime yol göstericilik yapılması,*
- *KRY faaliyetlerinin koordine edilmesi,*
- *Risklere yönelik konsolide raporlama yapılması,*
- *KRY çerçevesinin işletilmesi ve geliştirilmesi,*
- *KRY sisteminin oluşturulmasına liderlik edilmesi,*
- *Yönetim kurulunun onayına sunulacak KRY stratejisinin geliştirilmesi,*

İç denetim faaliyetinin üstlenmemesi gereken faaliyetler;

- *Kurumun risk iştahının belirlenmesi,*
- *Risk yönetimi süreçlerini yürürlüğe koymak,*
- *Risklerin yönetildiğine (iç denetim birimince) dair güvence vermek,*
- *Risklerin nasıl giderileceğine dair kararlan almak,*

[34] M. Ali Madendere ,(Çeviri / Derleme), **"Kurumsal Risk Yönetiminde İç Denetimin Rolü",** Ekim 2005,s.14. (Çevrimiçi: www.tide.org.tr)

- *Yönetim adına risklerin giderilmesi için gerekli önlemleri almak,*

- *Risk yönetimi sistemine ilişkin hesap verebilir bir pozisyonda olmak,*

Kurumun risk yönetimi süreçlerinin güçlendirilmesine sayısız şekillerde katkıda bulunması mümkün olmakla birlikte; iç denetçilerin üstlenmemesi gereken sorumluluk risk yönetimi sürecinin nihai sorumluluğunu almaktır. Kurum içerisinde risk yönetimi yönetim kurulu ve üst yönetimin sorumluluğunda olup bu sorumluluğu iç denetçilerin üstlenmeleri tarafsızlıklarım yitirmelerine yol açacaktır. Hatta risk yönetimi süreçlerinde danışman pozisyonunda yer alan iç denetçilerin belirli bir süre söz konusu sistemlerin denetiminde görevlendirilmemesi dahi söz konusu olacaktır. Aynı şekilde iç denetim yöneticisi danışmanlık kapsamında gerçekleştirilecek her bir faaliyetin iç denetim faaliyetinin tarafsızlık ve bağımsızlığına zarar verip vermeyeceğini değerlendirmesi gerekmektedir.

Son olarak değinilmesi gereken husus; etkili bir risk yönetimi kurmak isteyen kurumların ilk yapması gereken işlerden birisi olarak, iç denetim biriminin modernizasyonu ve risk odaklı bir denetim mantalitesiyle standartlara uygun denetim yapan bir iç denetim birimi haline getirilmesidir. Bir yandan son derece modem bir risk yönetimi sistemi varken diğer yandan sadece mevzuata uyum odaklı bir iç denetim sistemi birbirlerine uyum sağlamayacakları gibi bu tür bir iç denetim sisteminin KRY sisteminin kurulmasına bir katkı sağlayamayacak, bir sonraki aşamada da söz konusu sistemin denetimini yapması da mümkün olmayacaktır. Diğer bir deyişle KRY sistemi uygulamaya başlanmadan önce sistemin tanımının diğer tüm birimlerden önce iç denetim birimine yapılması ve iç denetim sisteminin KRY sürecine katkı sağlayacak ve denetleyecek bir yapı ve beşeri sermayeye sahip olması sağlanmalıdır.[35]

2120-2 No'lu uygulama önerisi kurumsal risk yönetimine ilave olarak iç denetim faaliyetinin kendisine yönelik risklerin nasıl yönetileceği hususunda şu önerilerde bulunmaktadır;[36]

- *İç denetimin rolü ve önemi çok büyümüştür ve önemli paydaşların (yönetim kurulu, üst yönetim gibi) beklentileri de artmaya devam etmektedir. İç denetim faaliyetlerinin, finansal, operasyonel, bilgi*

[35] M. Ali Madendere ,(Çeviri / Derleme), **"Kurumsal Risk Yönetiminde İç Denetimin Rolü",** Ekim 2005, s.15.(Çevrimiçi: www.tide.org.tr)
[36] Uygulama Önerisi 2120-2

teknolojisi, yasal düzenleme ve stratejik riskleri kapsayan geniş yetkileri vardır. Aynı zamanda, birçok iç denetim faaliyeti, küresel iş piyasalarında kalifiye personel bulunabilirliğiyle, artan ücret maliyetleriyle ve özel kaynaklara yönelik yüksek taleplerle ilgili zorluklarla karşılaşmaktadır. Bu etkenlerin bir araya gelmesi, bir iç denetim faaliyetinde yüksek risk seviyesinin ortaya çıkmasına sebep olmaktadır. Bunun sonucu olarak, iç denetim yöneticileri, iç denetim faaliyetlerine ve hedeflerine ulaşmaya yönelik riskleri göz önünde bulundurmalıdırlar.

- *İç denetim faaliyeti, risklerden muaf değildir. Kendi risklerini yönettiğinden emin olmak için gerekli önlemleri almalıdır.*

- *Yanlış güvence riskini tamamını yok etmenin bir yolu olmasa da, iç denetim faaliyeti, bu alandaki riski daha önceden tedbir alarak yönetebilir.*

- *Bir iç denetim faaliyetinin güven telkin eden itibarı, etkililiğinin önemli bir parçasını teşkil eder. Saygın görülen iç denetim birimleri yetenekli meslek insanlarını çekebilirler ve kurumlan için çok değerlidirler. Güçlü bir "marka" olmak, iç denetim faaliyetlerinin başarısını ve becerisini kuruluş içinde en üst noktaya çıkartır. Çoğu zaman, iç denetim faaliyetinin markası gücünü, uzun yıllar boyunca aksamadan çıkartılan yüksek nitelikli işlerden almaktadır. Maalesef bu marka, güçlü ve ters bir olayda birden yok olabilir.*

Bir iç denetim faaliyeti, yukarıda belirtilenlere benzer bir olayla karşılaştığında, İç Denetim Yöneticisi, olayın içeriğini gözden geçirmeli ve sorunun ana sebeplerini anlamalıdır. Bu analiz, oluşabilecek olumsuzlukları azaltmak için, iç denetim süreci ve kontrol sisteminde dikkate alınması gereken potansiyel değişikliklere karşı derinlikli bir bakış açısı getirir.

BÖLÜM II

RİSK YÖNETİMİ VE İŞLETMELERDE RİSK YÖNETİMİNE İLİŞKİN MODELLER VE ULUSLARARASI STANDARLAR

2.1.Risk Yönetimi ve Kurumsal Risk Yönetimi Kavramları

Risk genel olarak, organizasyonu bütünüyle etkileyebilecek olan mali kayıplar, etik olmayan davranışlar, güvenilirliğin zarar görmesi ve yasal gereklerle çalışma yönergelerine uygun olmama türünden bir olay ya da eylemin kurumu olumsuz bir biçimde etkileyebilmesi olarak ifade edilmektedir.[37]

Kurumsal Risk Yönetimi, kurumu etkileyebilecek potansiyel olayları tanımlamak, riskleri kuruluşun kurumsal risk alma yapısına uygun olarak yönetmek ve kurumun hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; stratejilerin belirlenmesinde de kullanılan sistematik bir süreçtir. Bu süreç, bir amaç olmayıp, sonuca ulaşmak için bir araç niteliğine sahiptir. Kurumsal Risk Yönetimi yaklaşımı esasen kurumun tüm faaliyetlerini kapsayan bir yönetim anlayışını ifade etmektedir.[38]

Geleneksel risk yönetimi kavramı ağırlıklı olarak finansal ve maddi zararlara yol açabilecek finansal faaliyetler veya doğal olaylara yönelik seçilen risk alanları, riskli görülen birim veya süreçler üzerinde spesifik iç kontrol önlemleri alınması yoluyla gerçekleştirilmiştir. Bu tür bir risk yönetiminin daha reaktif ve işlem süreci odaklı olduğu söylenmektedir.[39]

Ortaya çıkma sıklığının, zamanın ve şeklinin belirli olmaması sebebiyle risk, organizasyonlar tarafından zor ve karmaşık bir olgu olarak bilinmektedir.[40]Diğer bir deyişle her bir risk birbirinden bağımsız olarak ele alınmış ve her bir risk kendisine özgü kontrollerle giderilmeye çalışılmıştır. Bu aşamada da risk yönetiminin reaktif olduğunu söylemek doğru olsa da faaliyetler ve süreçlerin yanı sıra yönetsel unsurları da içermeye başladığını söylemek mümkündür.[41]

---

[37] Baran Özeren, **İç Denetim Standartları ve Mesleğin Yeni Açılımları,** Ankara, Sayıştay, 2000, s.42.
[38] TÜSİAD, Risk ve Değer Yönetimi Çalışma Grubu, **''Kurumsal Risk Yönetimi''**, Ankara, 2006. s.23.
[39] Protiviti Inc. **"Guide to ERM 2006''**, (Çevrimiçi:www.protiviti.com, Erisim: 12.05.2012)
[40] David McNamee, **Risk Based Auditing,** CA USA, Management Control Concepts Alamo, 1997, s.7.
[41] Protiviti a.g.e

Risk, organizasyonun amaçlarına ulaşma ve stratejilerini başarılı bir şekilde sürdürme kabiliyetini olumsuz yönde etkileyen bir tehdittir.[42] Bu tanım, risk ile ilgili şu özellikleri vurgulamaktadır:[43]

• Risk değişken bir tehdittir.

• Tehdit bir olayla ilgilidir.

• Olay meydana geldiğinde organizasyon hedeflerine ulaşamaz.

Kurumlarda kullanılan risk yönetim modelleri aşağıda sırasıyla açıklanmıştır.

2.1.1. KRY Modeli

Kurumsal Risk Yönetimi, "Enterprise Risk Management, ERM"[44] Committee of Sponsoring Organizations of the Treadvvay Commission (COSO) tarafından 1992 yılında geliştirilen "COSO İç Kontrol Bütünleşik Çerçeve" nin "Risk Değerlendirme,'' bölümünün detaylandırılması yoluyla geliştirilerek 2004 yılında yayımlanan ve kurumların faaliyetlerinde karşılaşabilecekleri tüm risklerin etkili ve sistematik bir şekilde tanımlanması, ölçülmesi, değerlendirilmesi ve giderilmesi konusunda kurumlara rehberlik sağlamayı amaçlayan bir modeldir.[45]

Bu modeli hazırlayan komisyona başkanlık eden kişi COSO kontrol modelinden farklı olarak bu modelin özellikle risklerin teşhis edilmesi, analizi ve yönetilmesi amacıyla hizmet ettiğini vurgulamakta ve modelin bir anlamda iç kontrolün kapsamını genişlettiğini belirtmektedir.[46]

COSO, Kurumsal Risk Yönetimi Çerçeve Raporunda kurumsal risk yönetimi şu şekilde tanımlanmaktadır;

"Kurumsal risk yönetimi, kurumun yönetim kurulu üyeleri, üst düzey yöneticileri ve diğer çalışanları tarafından etkilenen, strateji oluşturulması aşamasında ve bütün kurum boyunca uygulanan, kurumu etkileyebilecek olası tüm olayların tanımlanması

---

[42] Phil Griffiths, **Risk-Based Auditing**, England, Gower Publishing Limited, 2005, s.17.
[43] Phil Griffiths, s.17.
[44] COSO, Enterprise Risk Management, ERM, **''Integrated Framevvork, Application Techniques 2004'',** www.coso.org, s.3.
[45] Çetin ÖZBEK, **''İç Denetim''** , TİDE Yayınları , Yayın No:3 s.262 , İstanbul ,Ekim,2012
[46] John Flaherty, COSO, Enterprise Risk Management **, ''Integrated Framework**, **Executive Summary 2004''** (Çevrimiçi: www.coso.org, Erisim: 27.12.2012) s.4.

için tasarlanan ve kurum amaçlarının gerçekleştirilmesine yönelik makul bir güvence sağlamak amacıyla risklerin belirlenen risk iştahı içerisinde yönetilmesini sağlayan bir süreçtir"[47]

Bütün kurumlar belirsizlikle karşı karşıyadır ve yöneticilerin sorunu hissedarların hisse değerini artırırken aynı zamanda ne kadar risk alabileceklerine karar vermektir. KRY'in becerileri kurumların performans ve karlılık amaçlarının gerçekleştirilmesine yardımcı olur ve kaynak israfının önüne geçer. Kısaca KRY, kurumlara ulaşmak istedikleri yere ulaşmalarına ve buraya ulaşırken yol üstündeki sürpriz ve tehlikelerden kaçınmalarına yardımcı olur.[48]

KRY, COSO iç kontrol modelindeki 3 temel amaca kurumsal stratejiyi de dahil etmekte ve kurumun 3 boyutunu COSO kontrol kübüne benzer şekilde kurumsal risk yönetim kübüyle (Şekil-1) göstermektedir.

Şekil 1-KRY Kübü

(Kaynak:Çevrimiçi:http://kontrol.bumko.gov.tr/TR,2185/cosohakkinda.html, Erişim: 21.02.2013)

[47] COSO, Enterprise Risk Management, ERM, **''Integrated Framevvork, Application Techniques 2004'',** www.coso.org, s.4.
[48] COSO, Enterprise Risk Management **, ''Integrated Framework**, **Executive Summary 2004''** (Çevrimiçi: www.coso.org, Erisim: 27.12.2012)s.6.

Birinci boyut kurumun stratejik, operasyonel, finansal ve mevzuata uyum hedefleridir.

İkinci boyut örgütsel yapıyı ifade eder. Birimler veya ana fonksiyonlar bazında KRY adımlarının izlenmesini ifade eder. Üçüncü boyut KRY adımlarını ifade etmektedir.

Şekil-1 'de verilen küpte görüleceği üzere kurumun her faaliyet ve biriminde gerçekleştirilmesi gereken amaçlar için birbiriyle ilişkili 8 temel adımın atılması gerekmektedir. Bunlar;[49]

5. Kontrol Ortamı
6. Amaçların Belirlenmesi
7. Olayların Tanımlanması
8. Risklerin Değerlendirilmesi
9. Risklere Karşılık Verme
10. Kontrol Faaliyetleri
11. Bilgi ve İletişim
12. Gözlemleme 'dir.

COSO İç kontrol modelinde olduğu gibi KRY' in her üç boyutu da birbiri ile yakın ilişki içerisindedir. Yukarıda yer alan yaklaşım KRY' in bir bütün olarak değerlendirilebileceği gibi bileşenlerine ayrılarak bir alt birimi etkileyen bir hedefin KRY aşamalarından herhangi birindeki halini incelemeye izin verecek şekilde izlenmesine imkan verecektir.

Yukarıda verilen Şekil-1 'deki bileşenler aşağıda açıklanmıştır.[50]

Kontrol Ortamı; Risklerin kurumda çalışan kişiler tarafından nasıl görüntülenmesi ve yönlendirilmesi gerektiğine dair bir temel oluşturur. İç ortam kurum ile ilgili risk yönetimi felsefesi, risk kapasitesi, dürüstlük etik değerler ve faaliyet gösterilen çevre gibi kavramları içerir.

[49] COSO, Enterprise Risk Management, ERM, **''Integrated Framevvork, Application Techniques 2004'',** www.coso.org, s.21.

[50](Çevrimiçi:www.sgb.gov.tr/MaliyeUzmYrdArasRaporlari/Maliye%20Uzmanlığı%20Araştırma%20Raporları/Kurumsal%20Risk%20Yönetimi%20Işılda%20ARSLAN.pdf, s.29.,Erişim: 12.05.2013)

Amaçların Belirlenmesi; Kurumsal risk yönetimi kurumun vizyonu ve misyonu ile uyumlu olan ve bu iki unsuru destekleyen strateji ve amaçların belirlenmesine yardımcı olmak üzere tasarlanmış bir süreçtir. Ayrıca bu strateji yürütülürken karşılaşılacak risklerin kurumun risk kapasitesi sınırları içinde olmasını sağlayan bir süreçtir. Amaç belirleme sürecinin bu iki parametre misyona ve vizyona uyumlu olma ile amaçların onlara ulaşılmak için karşılaşılacak risklerin risk kapasitesi içinde kalmasını sağlayacak seviyede koyulması dikkate alınarak yürütülmesi gerekir.

Olayların Tanımlanması; Kurumların amaçlarının gerçekleştirilmesini etkileyebilecek içsel ve dışsal olayların fırsat ve tehditler ayrıştırılarak tanımlanması gerekmektedir. Kurumun hedeflerine ulaşmasını etkileyen, risk ve fırsatlar arasında değişen iç ve dış olaylar tanımlanır.

Risk Değerlendirme; Riskler tanımlandıktan sonra bunların kurum üzerindeki olası etkilerinin ve meydana gelme olasılıklarının değerlendirilmesi gerekir. Riskler, nasıl yönetilmeleri gerektiğinin belirlenmesine destek oluşturmak amacıyla gerçekleşme olasılık ve yaratacakları etki dikkate alınarak analiz edilirler. Riskler doğal ve artık riskler olarak değerlendirilirler.

Risklere Karşılık Verme; Yönetim kurumun risk toleransı ve risk iştahı ile uyumlu risk yönetimi araçları geliştirmek suretiyle risklerden kaçınma, kabul etme, azaltma veya paylaşma risklere yönelik uygun karşılıklar geliştirir.

Kontrol Faaliyetleri; Kontrol faaliyetleri, riske verilecek karşılıkların etkili bir biçimde yerine getirilmesi, devam eden risklerin risk kapasitesi sınırları içinde yönetilmesi ve kurumun yürürlükteki yasa ve yönetmeliklerle uyumunun sürekli sağlanmasına yardımcı olmak için yerleştirilen politika ve prosedürlerdir.

Bilgi ve İletişim; Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır, ele geçirilir ve iletilir. Buna ilave olarak etkili iletişim daha geniş bir anlamda bilginin, yukarıdan aşağıya, aşağıdan yukarıya ve kurum boyunca iletilmesiyle oluşur.

Gözlemleme; Kurumsal risk yönetiminin bir bütün olarak izlenmesi ve gerektiğinde değişikliklerin yapılmasıdır. İzleme sürekli bir şekilde yapılan yönetsel bir faaliyet veya sadece risk yönetiminin izlenmesine özgü spesifik değerlendirmeler veya her ikisi bir arada yapılabilir.

KRY'in başarıyla uygulanabilmesi için her bir bileşeninin doğru bir şekilde planlanması ve uygulanması gerekmektedir. Ancak bu uygulama kurumların faaliyet alanına, büyüklüğüne göre değişebilecektir. Büyük ölçekli kurumlarda daha formel olabileceği gibi küçük ölçekli kurumlarda daha az formel veya daha küçük bir yapıda olabilir. Önemli olan sekiz alt adımın sırasıyla izlenmesi ve etkili bir şekilde çalışmasının sağlanmasıdır. KRY'in yukarıda bahsedilen alt parçaları aynı zamanda KRY modelinin etkili bir şekilde çalıştığının değerlendirilmesi için gerekli kriterleri de sağlamaktadır. Diğer bir deyişle kurum içerisinde uygulanan KRY uygulamaları modelde yer alan her bir parça ile karşılaştırılarak kurumun etkililiğini ölçebilmektedir.

Başarıyla uygulanan bir KRY modeli kurumun risk yönetimi maliyetlerinin düşmesine, iş performansının artırılmasına ve kurumun rekabet avantajı geliştirmesine yardımcı olacaktır.

Risklerin belirlenmesi ve değerlendirilmesi yolu ile yapılan planlama, iç denetimi reaktif kontrole dayalı olmaktan çıkarıp, riske dayalı ve proaktif bir fonksiyona dönüştürmektedir. Etkin bir risk değerleme ile iç denetçi mevcut sorunlara çareler bulmakla kalmayacak, problemleri önceden görerek organizasyonu kayıplardan veya kaçırılan fırsatlardan korumada önemli bir rol oynayacaktır.[51]

KRY Modelinin alt bileşenlerinin Anonim Şirketlerde nasıl uygulanabileceğine dair değerlendirmelere Beşinci Bölümde yer verilmektedir.

Aşağıda KRY dışında kalan risk yönetimi standartlarına kronolojik olarak kısaca değinilecek olup ardından KRY kübünü oluşturan tüm bileşenler bütün bir süreç içerisinde ayrıntılarıyla incelecektir.

2.1.2. ISO 31000 Uluslararası Standartlar Kurumu-Risk Yönetimi Standardı

ISO 31000 Kod No'lu Risk Yönetimi Standartlar Seti, 31000-Prensipler ve Uygulama Rehberi, IEC 31010 Risk Yönetimi- Risk Değerlendirme Teknikleri ve ISO/IEC 73: Risk Yönetimi-Sözlük dokümanlarından oluşan ve her ülke, kurum ve riske uygulanabilecek bir standartlar seti olarak 2009 yılında yayımlanmıştır. Söz konusu standartlar geniş bir komite tarafından geliştirilmekle birlikte; uzun yıllardır

[51] A. Rıza Eşkazan, "Yeni Yasal Düzenlemeler Işığında İç Denetim", **İç Denetim,** Yaz 2005, s.32

Avustralya ve Kanada otoriteleri tarafından geliştirilen risk yönetimi uygulamalarının ve prensiplerinin etkisi bulunmaktadır.[52]

ISO 31000, risk yönetimini bir çerçeve halinde sunmaktadır. Buna göre; risk yönetimi çerçevesi "kurum çapında risk yönetiminin tasarlanması, uygulanması, izlenmesi, gözden geçirilmesi ve sürekli bir şekilde iyileştirilmesi için örgütsel düzenleme ve bir temel sağlayan bileşenler seti" dir. Risk yönetimi çerçevesi, kurumun bütün stratejik ve operasyonel politika ve uygulamalarına yerleştirilmelidir. Örgütsel düzenlemeler planlamayı, ilişkiler setini, hesap verebilirliği, kaynakları, süreçleri ve faaliyetleri içerir. Çerçevenin ilk önemli unsurunu yönetim kurulunun ve üst yönetimin kararlılığı ve talimatları oluşturmaktadır. ISO 31000'e göre; yönetim kurumun risklere karşı tavrını ortaya koymalı, yönetim kurulu ise riske yönelik tavırları kurum sahiplerinin menfaatleri ile uyumlu olduğunu belirlemekle yükümlü olmalıdır. Sonraki adımlar ise, sırasıyla çerçevenin tasarlanması, risk yönetiminin uygulanmaya konması, çerçevenin izlenmesi ve gözden geçirilmesi ve son olarak çerçevenin iyileştirilmesidir.[53]

ISO 31000, risk yönetimi süreçlerini ise, yönetimin belirlediği ortam içerisinde gerçekleştirilen risk değerlendirme ve riskin giderilmesi aşamaları olarak iki ana süreç halinde tanımlamaktadır. Bu iki ana sürece ilişkin geri besleme mekanizmaları ise risk yönetiminin performansının değerlendirilmesi ve izlenmesi ile iletişim ve istişare şeklinde iki ana yöntem olarak tanımlanmaktadır. İki ana süreçten biri olan risk değerlendirme, risk tanımlaması, risk analizi ve risk ölçümlemesi olarak üç alt bölümden oluşmaktadır. Riskin giderilmesi ise söz konusu risklerin giderilmesi amacıyla uygulanan uygun iç kontrol önlemlerinin seçilmesi ve uygulanmasını ifade etmektedir.[54]

2.1.3. AS/NZS 4360 Avustralya/Yeni Zelanda Risk Yönetimi Standardı

AS/NZS 4360 Risk Yönetimi standardının özelliği ilk geniş kapsamlı risk yönetimi standardını oluşturmasıdır. İlk versiyonu 1995 yılında geliştirilmiş olup 1999 ve 2004 yıllarında revize edilmiştir. Son olarak 2009 yılında AS/NZS 4360: ISO 31000

[52] Özbek, a.g.e. , s.268.
[53] Özbek, a.g.e. , s.269.
[54] Özbek, a.g.e. , s.270.

ile son şeklini almıştır. Son aşamada yeni bir revizyon yerine ISO 31000'in adapte edilmesi kararlaştırılmıştır. Söz konusu standartta risk, [55]

"Kurum hedefleri üzerinde etkisi olabilecek bir şeyin olması ihtimali" olarak tanımlanmaktadır. Risk yönetimi ise "*yönetim, olumsuz etkilerle mücadele ederken potansiyel fırsatların değerlendirilmesi amacına yönlendirilen kültür, süreçler ve yapılardır. "* şeklinde tanımlanmaktadır.

2.1.4. BS 31100 İngiltere Risk Yönetimi Standardı

Ekim 2008 yılında Britanya Standartlar Enstitüsü tarafından yayımlanan Britanya'nın ilk risk yönetimi standardıdır. Risk yönetimine ilişkin genel bir çerçeve oluşturulmasının yanı sıra kurum hedeflerinin gerçekleştirilmesi, spesifik faaliyet veya alanlarda risklerin proaktif bir şekilde yönetilmesi, risk yönetimi faaliyetlerinin gözetiminin sağlanması, risk yönetimi stratejisine dair bir güvence sağlanması amaçlarıyla kullanılmaktadır. Standartlar seti risk yönetimi prensipleri, risk yönetimi genel çerçevesi, risk yönetimi süreci ve risk yönetimi faaliyetlerinin geliştirilmesi hususlarını kapsamaktadır.[56]

2.1.5. Federation of European Risk Management Associations (FERMA) Risk Yönetimi Standartları

1974 yılında kurulan FERMA, günümüzde çok sayıda sektörden 4200'ün üzerindeki üyesiyle risk yönetimi alanında bilgi ve deneyim paylaşımını hedefleyen en önemli kuruluşlardan birisi olup iki ana stratejik hedefi bulunmaktadır;[57]

- *Avrupa'da risk yönetimi, sigortacılık ve risk finansmanının gelişimini ve kullanımı koordine etmek, tanıtmak ve desteklemek,*
- *Risk yönetimi, sigortacılık ve risk finansmanı konularına Avrupa düzeyinde karar alma süreçlerinde önemli paydaş olmak.*

Ülkemizi 2009 yılında kurulan Kurumsal Risk Yönetimi Derneği'nin[58] temsil ettiği FERMA, Risk Yönetimi Standartları İngiltere'de Institute of Risk Management

[55](Çevrimiçi:http://www.esisac.com/publicdocs/assessment_methods/AppC_AS-NZS_4360_2004.pdf , (Erişim:11.12.2012), s.1.
[56] Özbek, a.g.e. , s.270.
[57] Özbek, a.g.e. , s.270.
[58] Kurumsal Risk Yönetimi Demeği, (Çevrimiçi:www.kryd.org, Erişim:25.01.2013)

(IRM)[59], The Association of Insurance and Risk Managers (AIRMIC)[60] ve The National Forum For Risk Management in The Public Sector (ALARM)[61] tarafından oluşturan risk yönetimi standartlarını kabul ederek uyarlamaktadır. Söz konusu risk yönetimi standartlarının amaçları;[62]

- *Kullanılan kelimelerle ilgili terminoloji,*
- *Risk yönetiminin yürütülebileceği bir süreç,*
- *Risk yönetimi için örgütsel yapı,*
- *Risk Yönetiminin amacı konularında fikir birliği oluşturmaktır.*

2.1.6. Yeni Risk Değerlendirme Yöntemleri

Piyasalar, büyüme potansiyeli doğrultusunda risk alınmasını, karlı bir büyüme elde edilmesini ve bu büyümenin sürdürülmesini ödüllendirmektedir. Bu amaçla yasal uyumlulukla mücadelesini tamamlamış ileri görüşlü yeni risk yönetim stratejileri geliştirilmeye başlanmıştır. Aralarında yönetimin stratejik planlarının, gelir hedeflerini saptama ve onaylamanın, yönetişim, risk yönetimi ve uyumlulukta etkinlik ve verimliliği arttırmanın da bulunduğu değer odaklı risk yönetim etkinlikleri giderek ön plana çıkmıştır.

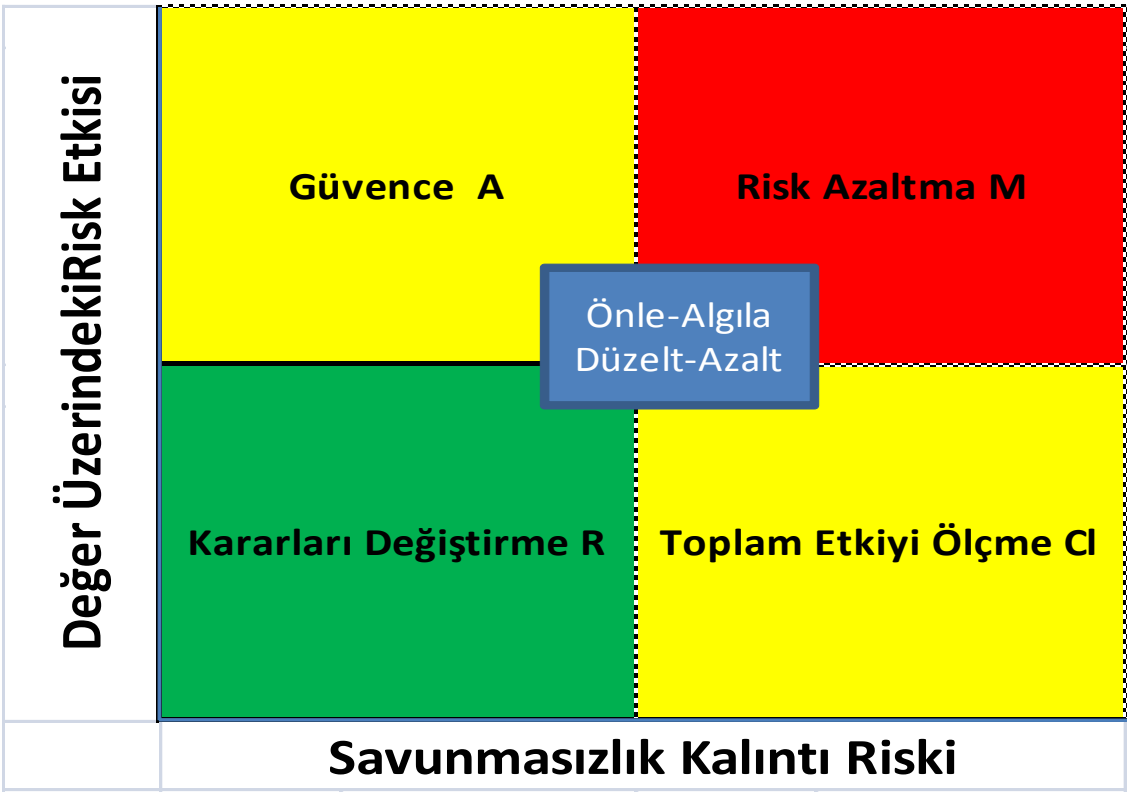
Yukarıda anlatılmaya çalışılan risk yönetim standartlarından başka henüz tam anlamıyla uygulamaya konulmamakla birlikte yeni çağdaş yaklaşım modelleri geliştirilmeye başlanmıştır. Bir bağımsız denetim şirketinin kurumsal müşterileri için geliştirdiği modelin unsurları aşağıda Şekil-2 üzerinde açıklanmıştır. [63]

2.1.6.1.Savunmasızlıkları Belirleme

Birçok şirket risk yönetim programlarını belirli olumsuz olayların gerçekleşme olasılığına dayandırır. Bu yaklaşım, özellikle iç denetim mesleğinde ve finansal hizmetler ve enerji sektörlerinde yaygın olarak kullanılmaktadır.

---

[59] Institute of Risk Management (IRM), (Çevrimiçi: www.theirm.org,) Erişim:25.01.2013)
[60] The Assodation of Insurance and Risk Managers (AIRMIC), (Çevrimiçi: www.airmic.com Erişim:25.01.2013
[61] The National Forum For Risk Management in The Public Sector (ALARM),(Çevrimiçi: www.alarm-uk.org Erişim: 25.01.2013)
[62] Özbek, a.g.e. , s.271.
[63] Cüneyt Kırlar,**"Risk Zeka Serisi''**, (Çevrimiçi:www.deloitte.com.tr/RiskZekasiSerisi-3,Erişim:14.04.2013) s.8.



Şekil 2- Yeni Risk Değerlendirme Yöntemi

(Kaynak: Çevrimiçi:www.deloitte.com.tr ,Erişim: 12.05.2013)

Ancak, olasılıklara dayalı risk değerlendirmeleri her zaman yeterli olmamaktadır. Son yıllarda yapılan araştırma çalışmaları şunu göstermektedir: büyük değer kayıpları genellikle etkisi yüksek, gerçekleşme olasılığı düşük olaylardan kaynaklanmaktadır.

Eğer üst yönetim sadece hem etkisi, hem de gerçekleşme olasılığı yüksek olaylara yönelik risklerin azaltılması konusuna yoğunlaşıyorsa, iç denetim, kaynakların yeterli bir kısmının gerçekleşmeleri halinde şirketi olumsuz etkileyebilecek fakat savunmasızlığı yüksek olan risklere aktarılmasının gerekliliğini savunmalıdır. Bir risk yapılan iş ile bağlantılı ve oldukça yüksek bir etkiye sahipse, gerçekleşme olasılığına bakılmaksızın hedef alınmalıdır.

Bu durum, özellikle değer yaratma ile bağlantılı riskler için geçerlidir. Zaman ufku ne kadar büyük olursa, belirsizlik de o kadar büyük olur ve olasılıklara dayalı tahminler de o kadar geçersiz hale gelir.

Güvence

Şekil 2'deki "A" bölümüne düşen riskler için, bu riskleri önlemek, algılamak, düzeltmek ve azaltmak için gerçekleştirilen kontroller aracılığı ile, ilgili risklerin kurumun risk iştahı sınırlarında etkili ve verimli bir şekilde yönetildiğine dair makul bir güvence vermesi kurum yönetiminden beklenmelidir. İç denetimin bu noktadaki görevi ise, yönetimin bu süreçteki faaliyetlerinin etkinliğine ve raporlarına güvenilebileceğine dair ikincil bir güvence vermektir.

Yönetimin makul değil sadece sınırlı güvence verdiği durumlarda, ki bu durumlar mevcut kontrollerin yalnızca bir kısmı etkin olarak çalıştığında oluşmaktadır, iç denetim, etkin oldukları varsayılan kontrolleri denetlemeli, etkin olmayan kontrollerin ise geliştirilmelerini desteklemelidir.

Azaltma

"M" bölümüne düşen riskler için yönetim, bu riskleri yönetmek için tesis edilmiş kontrollerin etkin olup olmadıklarına veya maruz kalınan riskin şirketin risk iştahı sınırlarında bulunup bulunmadığına dair herhangi bir güvence verememektedir. Bu gibi durumlarda, yönetim savunmasızlığın azaltılması gereken riskleri ele almalı, iç denetim ise söz konusu riskleri azaltacak iyileştirme planlarının hazırlanmasına yönelik tavsiyelerde bulunmalı ve planların ilerleyişini de takip edecek çalışmalar geliştirmelidir.

Kaynakları Değiştirme

"R" bölümüne düşen riskler için iç denetim, bu riskleri yönetmek için tesis edilmiş kontrollerin etkinliğini test etmenin yanı sıra kontrolleri verimlilik açısından da değerlendirmeli ve yönetime verimliliği arttırmak için önerilerde bulunmalıdır.

Toplam Etkiyi Ölçme

Son olarak, "CI" bölümüne düşen riskler için, iç denetim bu risklerin, etkileşimlerini ve oluşabilme sıklıklarını da göz önüne alarak, aynı anda oluşmaları durumundaki toplam etkilerini değerlendirmeli ve ölçmelidir.

2.1.6.2.Riskleri Uyumlu Hale Getirme

Risk yönetimi yeni bir şey değildir. Aslına bakılırsa, birçok şirkette çok sayıda sofistike risk yönetim uygulamaları zaten mevcuttur. Kredi riskini finans departmanları, güvenlik ve gizlilik riskini BT departmanları yönetir. Ancak, bu risk uzmanları genellikle örgütsel veya fiziksel olarak izole bir şekilde çalışır, aynı iş terimlerini kullanmaz ve riskleri farklı ölçütler kullanarak ölçerler.

Doğal olarak riskler izole edilmiş halde değildir. Bir gizlilik riski kısa bir süre içerisinde bir itibar riskine, bir dava riskine ve bir finansal riske dönüşebilir. Ayrıca, Risk Zekası'nın kurumdaki uzman silolar arasında paylaşılabilmesi için gerekli haberleşmeyi sağlayarak, ortak bir risk dili geliştirerek, riskin saptanma, değerlendirilme ve ölçüm yöntemlerini uyumlu hale getirerek bir katalizör ve tetikleyici görevi de görebilmek mümkündür. Örneğin, günümüzde işletmelerde birden fazla risk ve kontrol öz değerlendirme süreci var ise, bu sayıyı azaltmak, yapılan değerlendirmeleri birleştirmek ve sonuç olarak daha iyi istihbarat elde etmek şirketler açısından faydalı olacaktır.[64]

2.1.6.3.Riskleri Koordine Etme

Risk Zekası'na sahip olma sürecinde organizasyonel birimler arasındaki boşlukları kapama süreci çok aşamalıdır ve ortak bir yönetişim, risk ve uyumluluk çerçevesi geliştirilmesini gerektirir. Yapılması gereken ilk şey, risk yönetimi için ortak bir dil tesis edilmesi, ve ilkeler, uygulamalar ve raporların standartlaştırılacağı uyumlu hale getirme sürecidir. Kurum bünyesindeki roller ve sorumluluklar, boşluklar ve çakışmaları tespit edebilecek bir şekilde gözden geçirilmeli ve netleştirilmelidir. Bu süreç, risk etkileşimlerini daha iyi anlamak ve yönetmek için bir portföy görünümü ortaya koyabilecek ve şirket içerisindeki tüm risk uzmanlarının çalışmalarının güvenilirliğini artırabilecektir.[65]

[64] Kırlar, a.g.e, s.9.
[65] Kırlar, a.g.e, s.10.

Bir sonraki adım olan 'senkronizasyon' daha gelişmiş öngörme, hazır olma, ilk tepki ve kurtarma süreçleri için departmanlar arası koordinasyonu kapsar. Farklı gruplar, koordine edilmiş iş akışları geliştirerek, bilgi taleplerinin zamanlamasını koordine edebilirler. Risk yönetimi sürecinde oluşabilecek aksamaları ve kesintileri engellemek için iş yükü talepleri düzenlenmelidir.

Son süreç 'rasyonelleştirme' sürecidir. Bu süreç, diğer birim yöneticileri ile birlikte çalışan bir İç Denetim Yöneticisinin değerlendirme, test ve raporlamaya yönelik mükerrer çalışmaların azaltılmasına veya önlenmesine yardımcı olabileceği bir alandır. Bu amaca genellikle kısmen mevcut teknolojiyi daha iyi kullanarak veya yeni bir teknoloji kullanmaya başlanarak ulaşılabilir. Önceki süreçlerde olduğu gibi, rasyonelleştirme süreci de şirketin katlandığı gider yükünün azaltılmasını sağlayacaktır.[66]

Danışmanlık hizmeti ile yöneticiler, organizasyondaki süreçlerde meydan gelen problemlere çözüm bulma, süreçlerin yeniden yapılandırılması ve sistemlerin geliştirilmesi gibi konularda iç denetçilerden öneriler almakta ve bu önerileri dikkate almak suretiyle ileride ortaya çıkması muhtemel sorunların da önüne geçme imkanı bulmaktadırlar.[67]

2.2.KURUMSAL RİSK YÖNETİMİ (KRY) UYGULAMA SÜRECİ

KRY' in tanımı COSO çerçevesinde şu şekilde verilmekteydi;[68]

"Kurumsal risk yönetimi, kurumun yönetim kurulu üyeleri, üst düzey yöneticileri ve diğer çalışanları tarafından etkilenen, strateji oluşturulması aşamasında ve bütün kurum boyunca uygulanan, kurumu etkileyebilecek olası tüm olayların tanımlanması için dizayn edilen ve kurum hedeflerinin gerçekleştirilmesine yönelik makul bir güvence sağlamak amacıyla risklerin belirlenen risk iştahı içerisinde yönetilmesini sağlayan bir süreçtir."

Halka açık anonim şirketlerin kurulması öngörülmekte olup zorunluluğun karşılanmasında şirketlere herhangi bir model önerilmemektedir.

---

[66] Kırlar, a.g.e, s.11.
[67] Gerrit Sarens, ve Ignace De Beelde, "Contemporary internal auditing practices: New Roles and Influacing Variables. Evidence from exented case studies", **Working Paper**, (October 2004) s.273.
[68] Özbek, a.g.e. , s.273.

İç denetim süreci, işletme içinde kurmaylık görevini üstlenmiş iç denetçiler tarafından yürütülür. İç denetçiler, organizasyon bünyesindeki iç denetim hizmetini gerçekleştirmek üzere işletme tarafından istihdam edilmiş kişilerdir. İç denetçilerin; performansı, etkinliği ve farklı faaliyet ve departmanların tanımlanan yönetsel politikalara uyumunu değerlendirmesi ve bunu yaparken de bağımsız bir şekilde hiçbir merciinin etkisinde kalmamaları beklenmektedir.[69]

Risk yönetimi kurumsal yönetişim için uygun bir ortam sunarak, pay sahiplerine ve işletmeye taraf olan diğer gruplara, yatırımlarının karşı karşıya bulunduğu risklerin temsilcileri olan yönetim kurulu tarafından farkında olunduğu ve işletme yönetimi tarafından sistematik olarak yönetildiği mesajını verir.[70]

Risk yönetimi süreçlerinde yönetim kurulu, kurum stratejisinin belirlenmesinin yanı sıra, bu stratejiye uygun temel hedeflerin açık ve anlaşılır bir şekilde ortaya konulması, kurum içi etik ve çalışma ortamının şekillendirilmesinde önemli roller üstlenebilir. KRY'in oluşturulmasında yönetim kurulu aşağıda açıklanan rolleri üstlenebilecektir.[71]

- *Üst yönetimin etkin bir risk yönetimi sistemi kurduğunu izlemek,*
- *Kurumun risk iştahına uyulduğunu izlemek,*
- *Kurumun risk portföyünü izlemek ve risk iştahına uyumlu olup olmadığı nı göz önünde bulundurmak,*
- *Önemli risklerden haberdar olmak ve üst düzey yöneticilerin gerekli önlemleri alıp almadığını izlemek,*

TTK ile öngörülen "Risklerin Erken Saptanması ve Yönetilmesi Komitesi" yönetim kurulu üyelerinden oluşabileceği gibi bir yönetim kurulu üyesinin başkanlığında uzmanlardan ve üst düzey yöneticilerden olabilir veya tamamen uzman ve üst düzey yöneticilerden oluşabilir. Söz konusu komitenin risk yönetimi faaliyetlerine ilişkin görevlerinin şu şekilde belirlenebileceği düşünülebilir;[72]

---

[69] Ersin Güredin, ‘’**Denetim’’**, 10.Baskı, İstanbul, Beta, 2000, s.15.
[70] Spencer Pickett, **The Internal Auditing Handbook**, 2nd Edition, John Wiley & Sons, 2003,s.176.
[71] H.Abdullah Kaya**, “İç Denetim”** Bütçe ve Mali Kontrol Genel Müdürlüğü Maliye Başkanlığı, (Çevrimiçi: http://maliyesempozyumu.pamukkale.edu.tr/Abdullahkaya.pdf,Erişim:14.09.2012) s.6.
[72] Paul Sobel, **‘’Internal Auditing’’**,2007.s.21. den aktaran Özbek, **İç Denetim**, s.275.

- *Yönetim kurulunca kurumun risk iştahının belirlenmesine yardımcı olacak verilerin yönetim kuruluna sunulması ve bu konuda yönetim kuruluna teknik destek sağlanması,*
- *Kurumun tüm faaliyetlerinin yönetim kurulunca belirlenen risk iştahı sınırları içerisinde olduğunun izlenmesi,*
- *Yönetim kurulunca belirlenen hedef doğrultusunda ve sınırlar içerisinde risk yönetimi birimine gerekli rehberliğin sağlanması,*
- *Kurum içerisinde yönetim kurulunca oluşturulacak risk yönetimi kültürünün oluşmasına katkı sağlanması,*
- *Risk yönetimi faaliyetlerine ilişkin kurumun uymakla yükümlü olduğu mevzuat hükümlerine üst düzey yöneticiler ve tüm kademe çalışanlarca tam uyumun sağlandığının izlenmesi,*

Etkili bir iç denetim fonksiyonunun hem üstlenmesi ve hem de üstlenmemesi gereken roller aşağıdaki şekilde gruplandırılmıştır.[73]

KRY KAPSAMINDAKİ TEMEL İÇ DENETİM ROLLERİ	ŞARTLI OLARAK ALINABİLECEK İÇ DENETİM ROLLERİ	İÇ DENETİMİN ÜSTLENMEMESİ GEREKEN ROLLER
Risk yönetimi süreçleri konusunda güvence verme Risklerin doğru şekilde ölçülüp değerlendirildiği konusunda güvence verme Risk yönetimi süreçlerini ölçüp değerlendirme Önemli risklerin raporlamasını değerlendirme Önemli risklerin yönetilmesini gözden geçirme	Risklerin tanımlanmasına, ölçülüp değerlendirilmesine yardım etme Riskler konusunda yönetimi eğitme ve yetiştirme KRY faaliyetlerini koordine etme Risklerin raporlamasını konsolide etme KRY çerçevesini yürütme ve geliştirme KRY'nin oluşturulmasına öncülük etme Yönetim kurulunun onayına sunulacak risk yönetimi stratejisini geliştirme	Risk İştahını tesis etme Risk yönetimi süreçlerini kuruma empoze etme Riskler konusunda yönetim güvencesi Risk karşısında alınacak tutum konusunda karar verme Yönetim adına risk tutumlarını uygulama Risk yönetimi konusunda hesap verme

Şekil 3-KRY Sürecinde İç Denetim Rolü

73 Ahmet Borucu,'' **Kurumsal Risk Yönetimi Projelerinde Risk Değerleme Sürecinin İşlevi,**'' (Çevrimiçi:www.denetimnet.com , Erişim: 24.01.2013)

Uluslararası alanda yönetim kurulunun, kurumun risklerinin yönetilmesindeki sorumluluğunun denetim komiteleri ile birleştirilmesi konusunda ortak bir düşünce yoktur. ABD dahil birçok ülkede risk yönetimi için yönetim kurulu üyelerinden oluşan ve denetim komitesinden ayrı bir risk komitesi kurulabildiği gibi bu görev denetim komitesine de verilebilmektedir.[74]

TTK'nın 375. Maddesinde Yönetim Kurulunun devredilemez yetkileri arasında muhasebe, finansal denetim ve şirketin yönetiminin gerektirdiği ölçüde, finansal planlama için gerekli düzenin kurulması yer almaktadır. Bu maddeden risk yönetimi konusundaki yetkilerin devredilip devredilemeyeceği net olarak anlaşılmamaktadır. Maddenin gerekçesinde ise şu açıklama yer almaktadır;

"Komitenin sorumluluk sisteminin temelinde yer aldığı ve komitenin yönetim kurulu üyelerinden veya tamamen üçüncü şahıslardan kurulmasının mümkün olduğu" belirtilmektedir. Bu durumda madde de yer alan " sistemi çalıştırmak ve geliştirmekle yükümlüdür" ifadesinden risk yönetimi konusunda nihai sorumluluğun yönetim kurulunda olduğu anlaşılmaktadır. Ancak risk yönetimi gibi son derece yoğun zaman ayrılması ve operasyonel çaba harcanması gerektiren bir görevi günlük bazda yönetmesi mümkün olmayacağından, yönetim kurulunun, bu yetkisini kendi üyeleri arasından belirleyeceği üyeler aracılığıyla kuracağı bir komitenin gözetiminde izleyebileceği gibi kısmen veya tamamen üçüncü şahısları yetkilendirerek de yapabileceği düşünülebilecektir.[75]

Risk Yönetimi Birimleri; Komitenin doğrudan yönetim kuruluna raporlama yapması, bu komiteye bağlı görev yapan bir risk yönetimi biriminin olması sürecin işlerliğine katkı sağlayacaktır. Bu durumda kurumda bir risk yönetimi komitesi birde risk yönetimi birimi olması gerekecektir. Bu birimin risk yönetim komitesinin rehberliği altında doğrudan yönetim kuruluna bağlı olması idari açıdan yönetim kurulunun bu konudaki sorumluluğunu yerine getirmesi için gerekli ortamı ve raporlama düzenini sağlayacaktır.[76]

---

[74] Mehmet Tahir Özsoy **,"Risk Odaklı Denetim, ABD Uygulaması ve Türkiye Açısından Değerlendirilmesi",** Active Dergisi, Mart-Nisan 2009 s.1.
[75] Bakınız,TTK, Madde 375
[76] **''Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi",** Türkiye İç Denetim Enstitüsü Yayınları, No:3, İstanbul, 2005. s.125.

Bütün örgütsel yapı boyunca gerçekleştirilen çok sayıdaki risk yönetimi uygulamaları, risklere yönelik kontrol uygulamalarının gerektiği gibi çalışmasının sağlanması ve çalıştığının izlenmesi, alınması gereken ilave kontrol önlemlerinin hayata geçirilebilmesi üst düzey yöneticilerin alacağı kararlarla mümkün olacak, risk yönetimi komitesi ve üst yönetim bu kararlan alabilmek için risk yönetim biriminin raporlamasına ihtiyaç duyacaktır. Risk yönetimi birimleri kurum içerisinde gerçekleştirilen tüm KRY uygulamalarına ilişkin verilerin bir araya getirildiği, KRY uygulamalarının kurum içerisinde izlendiği ve koordine edildiği, risk raporlarının kurum içerisinde ilgili işlemlerin yapıldığı birimlerdir.[77]

Risk yönetiminin nihai amacı kurumun hedeflerinin gerçekleştirilmesini engelleyebilecek olası riskleri tanımlanarak olumsuz etkilerinin azaltılmasıdır. Her tür riskin belirli ölçüde kurumları olumsuz etkileme ihtimali bulunmaktadır. Yönetilebilen her risk kurumun önünü daha net görmesini, geleceğe ilişkin kararlarını daha doğru verilere dayanarak almasını ve sonuçta her türlü hedefine ulaşmasını kolaylaştıracaktır. Bir kurumun sayısız riski dikkate alması ve kendini buna hazırlamaya çalışması gereksiz maliyetlere yol açacağı gibi hedeflerine odaklanmasını da engelleyecektir. Burada amaç kesin bir çözüm almak değil kurum hedeflerine ulaşılmasına yardımcı olacak şekilde olabildiğince etkili bir sistem kurabilmektir.[78]

Kurumsal risk yönetimi konusunda uluslararası alanda muhtelif standart ve modeller söz konusudur. Şüphesiz; uluslararası modellerin Türkiye'de aynı şekilde uygulanması mümkün bulunmamaktadır. Her ülkenin kendisine özgü bir iş yapma kültürü, kurum organizasyon yapısı, işleyişleri ve insan kaynağı yapısı olacaktır. AB içerisinde bile farklı hukuksal sistemlere ve iş yapma kültürüne sahip ülkelerde aynı konuda birbirinden çok farklı uygulamalar görülebilmektedir. Tarihsel olarak farklı hukuk sistemlerine sahip Almanya ile İngiltere arasından iş yaşamına ilişkin düzenlemelerde çok önemli farklılıklar bulunmaktadır. Dolayısıyla, risk yönetimi gibi ülkemiz kültürüne dışarıdan girmiş bir uygulamanın kendi ülkemiz uygulamalarına uyarlanırken ülkemizin kendisine özgü kurallarının dikkate alınmasında fayda vardır.[79]

[77] Özsoy, a.g.e. s.2.
[78] Özsoy, a.g.e. s.4.
[79] Özsoy, a.g.e. s.5.

2.2.1. Kurumsal Risk Yönetim Sürecinin İşleyişi

Daha öncede açıkladığımız üzere KRY sisteminin başarılı bir şekilde kurulması için COSO komitesi, yönetim tarafından atılması gereken bazı adımların olduğunu açıklamaktadır. Ağırlıklı olarak ilk defa KRY sistemi kurulacak olan bir kurumda atılması gereken adımlar ve göz önünde bulundurulması gereken hususlar gerek COSO KRY modelinden esinlenilerek gerekse geleneksel proje yönetimi adımları dikkate alınarak sürecin aşamalarına aşağıda yer verilmiştir.[80]

Şekil 4- KRY Süreci

Bir kurumda, kurumsal risk yönetimi yani KRY sisteminin kurulması oldukça yoğun bir zaman, geniş bir ekip katılımı, uzmanlık ve maliyet gerektiren bir hususdur.

[80] COSO, **Enterprise Risk Management. ,Executive Summary Integrated Framework**, Application Techniques,2004, (Çevrimiçi: www.coso.org, Erisim: 27.12.2012) s.4.

Bu yüzden aşağıdaki adımların risk yönetim sürecinin etkililiği açısından takip edilmesi gerekmektedir.

- **Proje Ekibinin Oluşturulması ve Hazırlıklar:** Bütün önemli birim ve fonksiyonlardan yetkin ve tecrübeli kişilerin katılımı sağlanmalıdır. Söz konusu ekip KRY'in bileşenleri, kavram ve prensipleri konularında eğitilerek, KRY'i iyi bir şekilde anlamaları sağlanmalıdır. Bu eğitim aynı zamanda ekip üyeleri arasında ortak bir risk dilinin gelişmesine de yardıma olacaktır.

- **Üst Düzey Yönetimin Desteği:** Yönetim kurulunun kararlı talimatları ve üst düzey yönetimin desteği sistemin kurulabilmesi için olmazsa olmaz bir koşuldur. Bunun sağlanabilmesi için sık sık gelişmeler hakkında üst düzey yöneticilerin hazırlık toplantılarına katılmaları ve yönlendirici bilgi sağlamaları teşkilata sistemin kuruluşuna verilen önemin gösterilmesi açısından önem taşımaktadır.

- **Uygulama Planının Geliştirilmesi:** Bir sonraki aşamada önemli proje adımlarını, iş akışlarını, dönüm noktalarını, kaynakları ve zamanlamayı gösteren bir plan hazırlanmalıdır. Proje grubundaki roller ve sorumluluklar belirlenmeli ve bir proje yönetim sistemi uygulamaya alınmalıdır. Söz konusu plan, ekibin yönetilmesinde bir iletişim ve koordinasyon aracı olarak işlev görecek, diğer birimler ve çalışanlardan beklentilerin iletilmesi ve koordine edilmesi ile KRY'in kurumda adapte edilmesi ile kurumsal çapta meydana gelen değişikliklerin tartışılması için bir temel oluşturacaktır.

- **Risk Kültürünün Güçlendirilmesi:** Söz konusu ekip tarafından ilk yapılacak çalışmalardan birisinin kurum genelinde risk yönetiminden ne anlaşıldığının tespiti olacaktır. Ekip üyelerinin kendi aralarında oluşturdukları ortak risk dilinin tüm kurum çapında yaygınlaştırılması gerekli olacaktır. Bu amaçla grup üyeleri gerekirse risk ve risk yönetimi konusunda formel bir eğitime tabi tutulmalıdır.

- **KRY Adımlarının Gerçekleştirilmesi:** Bu aşamadan sonra KRY adımlarının gerek ekip çalışmasıyla gerekse diğer çalışanlarla uygulanması gerekecektir.

- **Uygulamanın Takip Edilmesi:** KRY'in her bir adımının gerçekleştirilme ve kurum içerisindeki uygulama süreçleri yakından takip edilmeli, gerekli hallerde iyileştirilmesi gereken süreçlere yönelik iyileştirme önlemleri alınmalıdır.

- **Raporlama Sisteminin Oluşturulması:** KRY sisteminin kurum içerisinde uygulanması sırasında gerek proje ekibi içerisinde, gerek proje çalışmaları hakkında tüm kurum çalışanlarına ve yönetim kurulu ile üst yönetime yeterli bilgiyi sağlayacak etkili ve yeterli bir raporlama sisteminin kurulması büyük önem taşımaktadır.

Daha öncede vurguladığımız gibi KRY sistemini uygulamak oldukça emek, zaman ve kaynak, bilgi ve deneyim gerektiren bir süreçtir. Dolayısıyla bu konunun getireceği faydalar ve yaratacağı ek maliyetler oldukça detaylı olarak yönetim kurulu ve üst yönetim tarafından değerlendirilmek zorundadır. Yönetim Kurulu ve üst düzey yöneticilerin risk yönetimi konusunda çok bilgili olduklarını varsaymak birçok durumda doğru bir yaklaşım olmayacaktır.

2.2.2. COSO - KRY Modelini Oluşturan Bileşenlerin Örgütsel Yapıya Adaptasyonu

Daha öncede açıkladığımız üzere COSO KRY modeli birbiriyle ilişkili aşağıda belirtilen sekiz bileşenden oluşmaktadır.

Kurum genelinde risk yönetimi sürecinin etkili bir şekilde işletilebilmesi bu sekiz bileşenin gerektiği gibi kurgulanmasına bağlıdır. Bunlar;

1. Kontrol Ortamı
2. Amaçların Belirlenmesi
3. Olayların Tanımlanması
4. Risklerin Değerlendirilmesi
5. Risklere Karşılık Verme
6. Kontrol Faaliyetleri
7. Bilgi ve İletişim
8. Gözlemleme ‘dir.

KRY ‘nin sekiz bileşeninin nasıl oluşturulması gerektiği alt başlıklar halinde açıklanmıştır.

2.2.2.1.Kontrol Ortamı

Kontrol Ortamı kurumun içerisinde faaliyette bulunduğu koşul, ortam, kurumun bir bütün olarak becerilerini, kaynaklarını ve sınırlarını ifade etmektedir. KRY de kontrol ortamına ilişkin açıklama şu şekildedir;[81]

"Kontrol ortamı çalışanların risk algılamasını etkileyen bir kurumun atmosferini yansıtır ve KRY'in diğer tüm bileşenleri için bir disiplin ve yapı sağlayarak bir temel oluşturur. İçsel ortam faktörleri bir Kurumun risk felsefesini, risk iştahını, yönetim kurulu tarafından sağlanan gözetimin seviyesini, dürüstlük ve etik değerlerini, çalışanların yeterlilik seviyesini, yöneticilerin yetki ve sorumluluk dağılımı, onları organize etme ve geliştirme usullerini içerir."

İçsel ortamın etkisi; Bir kurumun içsel ortamı risk yönetiminin nasıl hayata geçirildiği ve sürekli bir şekilde nasıl işletildiğini belirleyen bir etkiye sahiptir.

İçsel ortam hususunda KRY, iki ana konuya vurgu yapmaktadır. Birincisi, kurumun risk yönetimi felsefesi diğeri ise, dürüstlük ve etik değerlere olan bağlılıktır. Risk yönetim felsefesi KRY modelinde şu şekilde açıklanmaktadır;[82]

Bir kurumun risk yönetimi felsefesi, temel stratejilerin oluşumundan söz konusu stratejilerin günlük faaliyetlere uygulanmasına kadar karşılaşılan risklere karşılık verileceğini karakterize eden genel tavırlar ile paylaşılan değer yargılarının bir birleşimidir. Bu birleşim üst düzey yönetimin kurumu yönetirken yaptığı tüm işlerde kendisini gösterir. Yazılı politika belgelerinde, sözlü ve yazılı iletişimde ve karar alma da etkilerini gösterir. İster yazılı politika metinlerinde. davranış kalıplarında, performans göstergelerinde, istisna raporlarında vurgulansın isterse büyük oranda yöneticilerle yüz yüze iletişimde informel bir şekilde vurgulansın önemli olan yönetimin risk yönetimi felsefesini sadece sözlerle değil günlük eylemleriyle de göstermesidir. ”

[81] COSO, **Enterprise Risk Management. ,Executive Summary Integrated Framework**, Application Techniques,2004, (Çevrimiçi: www.coso.org, Erisim: 27.12.2012) s.5.
[82] COSO, **Enterprise Risk Management. ,Executive Summary Integrated Framework**, Application Techniques,2004, (Çevrimiçi: www.coso.org, Erisim: 27.12.2012) s.7.

KRY modelinde yukarıdaki ifade ile anlatılmaya çalışılan husus kurum içinde ne ölçüde bir risk farkındalığın olduğu, üst düzey yöneticilerden başlayarak tüm çalışanların günlük faaliyetlerinde risk yönetiminin ne ölçüde hesaba veya süreçlere dahil edildiğidir. Diğer husus ise, dürüstlük ve etik değerler olup KRY modelinde şu şekilde açıklanmaktadır;[83]

"*KRY'in etkinliği kurum faaliyetlerini yaratan, yöneten ve izleyen çalışanların dürüstlük ve etik değerlerinin üstünde olamaz."*

Yani çalışanlar ne kadar dürüst ise sistemde o ölçüde dürüst bir şekilde çalışır. Kurumun çalışma tarzını gösteren içsel ortam yönetimin felsefesi ve çalışma tarzının yansımasıdır. Bu ortamda değerle ülkeden ülkeye işletmeden işletmeye farklılık gösterebilir. Kurum kültürü, içinde birçok yönetsel süreç ve yöntem taşımakla birlikte; içinde bulunduğu toplumun değerlerinden de etkilenmektedir. [84]

Kurumsal kültürü oluşturan birçok unsur vardır. Kurum içi yönetim tarzı, çalışanların kurum içi kararlara katılma süreci, yönetim anlayışı çalışan gibi unsurlar kurumsal kültürün belirleyici öğeleridir. Bu kültürü yönlendiren ve ona şekil veren daha ziyade üst düzey yönetim yada karar alıcılarıdır. Ülkemizdeki işletmelerde yasalar yönetim kuruluna sorumluluklar yükler. Yöneticilerin tüm teşkilata verdiği mesajlar bu anlamda önemli ve etkilidir. Çünkü çalışanlar liderlerini taklit ederler. Yöneticilerin kendi kişisel menfaatlerini örgütün diğer paydaşlarının menfaatinin üstünde tutması kurumsal kültürü olumsuz etkileyebilir.

Üst düzey yöneticilerin kendi aralarındaki uyum seviyesi de teşkilata verilen bir mesajdır. Fonksiyonlardan kaynaklanan kurumsal pozisyonların dışında kişisel olarak güçlü yöneticilerin etki alanlarının kendi sorumluluk alanlarının sık sık dışına çıkması çalışanların hiyerarşik kanalları aşmalarına ve informel kanallara yönelmelerine yol açacaktır.

Bilgi paylaşımı kanallarının etkili, açık ve biçimsel olmaması kurum içi her gelişmenin önce informel kaynaklara yayılması, dedikodu ve söylenti mekanizmaları kontrol ortamını olumsuz etkilemektedir.

---

[83] COSO, **Enterprise Risk Management. ,Executive Summary Integrated Framework**, Application Techniques,2004, (Çevrimiçi: www.coso.org, Erisim: 27.12.2012)s.8.
[84] David Mc Namee, **Risk Based Auditing**, CA USA :Management Control Concepts Alamo, 1997 s.7

Dürüstlük, etik değerler ve çalışanların yeteneği, yönetimin felsefesi ve yönetim kurulunca sağlanan girdiler gibi faktörler vasıtasıyla çalışanların kontrol bilincini etkileyerek organizasyonun tarzını ortaya koyar.[85]

Yukarıda detaylarıyla açıklanan, çalışanların kendilerini uymakla yükümlü hissettikleri ve her kurumda hissedilmekle birlikte; çoğu zaman yazılı olarak bulunmayan psikolojik faktörler kurum kültürünün önemli birer parçaları olmaktadır. Söz konusu kurum kültürü ise, bir kurumda günlük işlerin nasıl yapıldığını, operasyonların nasıl gerçekleştirildiğini ve yönetildiğini belirleyen önemli bir unsur olacak hatta kurumun bir bütün olarak performansının en önemli belirleyicilerinden biri olacaktır.[86]

Risk yönetimi genel kavramları üzerinde "farklı düşünülmesi" halinde kurulmaya çalışılan sistemin işlemesinde sorunlarla karşılaşılacak bu da zaman içerisinde sistemin etkinliğini azaltacaktır. Çok büyük motivasyon ve kaynakla başlanan projelerin zaman içerisinde amacından uzaklaşması hatta rafa kaldırılması sık görülen bir yönetsel zaafiyet durumudur. Bu nedenle risk kavramı üzerinde herkesin mutabık kalacağı ve tüm teşkilatın aynı anlamı çıkaracağı bir ortak dil geliştirilmesi bir ön koşuldur. Kurumun veya kurumun önemli birimlerinden birinin, performansını veya karını azaltacağı endişesi uygulamada ayak bağı olacağı veya çok zaman alacağı gibi muhtelif kaygılarla veya tamamen kişisel nedenlerle "ben böyle bir risk görmüyorum demesi" sistemin işleyişini tıkayacaktır. Herhangi bir riskten sözedildiğinde tartışmalar artık onun bir risk olup olmadığı değil nasıl giderileceğin de yoğunlaşmalıdır.[87]

Ortak bir risk terminolojisi ve dili geliştirilmesi, risk kavramı ile neyin kastedildiği, nelerin risk olup olmadığı konularında kurum içi risk algılama kültürünün gelişmesinin ön koşullarından birisidir. Başarılı bir risk yönetiminin mevcut olduğu ve çalışanlar arasından güçlü bir risk algısının olduğu kurumların hedeflerini gerçekleştirme olasılığı diğerlerinden yüksek olacaktır. Güçlü bir risk algısının varlığı ise, üzerinde tüm kurum çapında mutabık kalınmış bir risk terminolojisi ve kültürünün varlığına bağlı olacaktır.

---

[85] E.Paul Lındow, ve D. Race Jill, Beyond Traditional Audit Techniques, **Journal of Accountacy Issues**, July2002, s.9.

[86] Fuat Öksüz, **"Sabacı Holding A.Ş Denetim Uygulamaları",** Türkiye İç Denetim Enstitüsü, İç Denetim Dergisi, Sonbahar –Kış 2005-2006, Sayı 13,s. 37.

[87] E. Michael Thomas, **"The Seven-Step Process to Risk-based Auditing",** *FSA Times* ,Second Quarter 2006 Vol 5 No 2, (Çevrimiçi:http://www.theiia.org/fsa/index.cfm?iid=223 Erişim:11.08.2012)

Ancak her konuda olduğu gibi bu konuda aşırıya kaçmamak da bir diğer ön-koşuldur. Şüphesiz, çok sıkı kurallara bağlanmış, aşırı detaylandırılmış ve yöneticilerin faaliyet alanlarını sınırlayan bir risk yönetimi sistemi yaratıcılığı ve inisiyatif kullanımını da sınırlayacağı gibi kurumu olası risklerden koruyarak hedeflerini gerçekleştirmesine yardımcı olmaya çalışırken bizatihi kendisinin kurumun önünde bir risk haline gelebileceği de göz önünde bulundurulmalıdır. Risk almak ticaret yapmanın ve birçok durumda faaliyette bulunmanın bir ön koşuludur.[88]

Risk kültürünün fazla abartılması, üst düzeyden başlayarak her kademe çalışanın sanki her an dünyanın başına yıkılması ihtimali varmışçasına çalışması veya risk yönetimi çalışanlarının kurumun en önemli işini yapıyormuş gibi davranmaları sistemi tıkayan diğer önemli bir unsur olacaktır. Her kurum, varlık nedenine uygun bir şekilde geliştirilen üst düzey stratejiler doğrultusunda faaliyette bulunmak, kar elde etmek ve önceden belirlediği performans hedeflerini gerçekleştirmek zorundadır.

Yönetim Kurulunun risk yönetimi komitesinin faaliyetlerini yakından izlemesi, üst yönetimden ve ilgili birimlerden düzenli bilgi ve rapor alması, üst yönetimin sistemin işlerliği yönünde aldıkları kararlan izlemesi, bu konuda büyük önem taşıyacaktır. Risk yönetimi gibi hassas konularda çalışanların kurumun risk yönetimi sistemi hakkında tereddüte düşmelerine sebebiyet verilmemeli, varsa tüm eleştiriler risk yönetimi komitesinde gündeme getirilerek çözüm aranmalı risk yönetiminin bugünü ve geleceği hakkında alt kademelere yanlış anlaşılabilecek mesajlar verilmemelidir.[89]

KRY sisteminin kurulacağı ortamın önemli unsurlarından birisinin kurum içerisinde açık ve anlaşılır bir risk kültürü ve ortak bir risk algılaması olduğuna yukarıda değinilmektedir. İkinci önemli husus, kurumun etik değerlerinin varlığı ve bu etik değerlere bağlılık seviyesidir. Etik değerler yıllar boyunca kurumun faaliyet tarzı veya çalışma felsefesi yoluyla yazılı olmayan bir şekilde geliştirildiği gibi yazılı ve formel de olabilir.[90]

COSO modelinde etik değerlerin önemi konusunda en çok vurgu yapılan konu üst düzey yöneticiler tarafından sergilenen yönetim şeklidir. Üst düzey yöneticilerin eşitlik, adalet, kurum değerlerine uyum ve bunların korunması konularındaki

[88] Öksüz, a.g.e ,s. 39.
[89] Öksüz, a.g.e ,s. 39.
[90] COSO, ERM ,a.g.e. s.5

hassasiyeti, risk alma seviyeleri, yönetim tarzı ve usulleri, alt kadroların nasıl davranması ve çalışması gerektiği konusundaki en önemli yol gösterici unsur ve motivasyon kaynağı olmaktadır.[91]

Türkiye Etik Değerler Merkezi kurum içi etik kültürünü oluşturan unsurlar hakkında önemli bilgiler aşağıdaki gibi açıklamaktadır.[92]

Kurum içi etik kültürünü oluşturan unsurlardan belki de en önemlilerden birisi tüm çalışanlarca yasal mevzuata uyum kadar kurumun kendi iç düzenlemelerine uyum konusunda gösterilen hassasiyettir. Her kurum kendi faaliyetlerini düzenleyen çok sayıda yasal düzenlemeye uymakla yükümlüdür. Her çalışan tarafından bu kurallara uyulması, uymama hallerinin nasıl raporlanacağı ve hangi önlemlerin alınacağının tüm çalışanlarca açık ve net bir şekilde bilinmesi, uyulmamanın yasal yaptırımlarının yanı sıra kurum içi disiplin yaptırımlarının net olması gerekmektedir. Kurum içi etik kurallara aykırı hususların raporlanabileceği veya üst düzey yöneticilerle tartışılabileceği adil bir iç iletişim sistemi kurulmalı, bu sistem aracılığı ile usulsüzlük veya aykırılıklara ilişkin raporlama yapan çalışanların kimlikleri gizli tutulmalı veya raporlamaları nedeniyle herhangi bir misillemeyle karşı karşıya kalmamaları garanti altına alınmalıdır.

Yukarıda örnekleri verilmeye çalışılan tüm bu hususlara yönelik kurum içi uygulamalar ve üst düzey yöneticiler ile tüm çalışanların bu konulardaki tutum ve davranışları kurum içi etik ortamını oluşturmaktadır. Bu kurallara uyulması veya uyumun sağlanması yazılı politikalarla olabileceği gibi bizzat yöneticilerin tavır ve davranışları ile de kendisini gösterebilir. Yaptırımlar konusundaki tavizsiz uygulamalar tüm çalışanlar tarafından uyulması gereken normlar olarak algılanacak ve kurum içi çalışma ortamının en önemli görünmeyen motivasyon aracı olarak kurumların günlük faaliyetlerinin her aşamasında ve her kademede kendisini hissettirecektir.

2.2.2.2.Amaçların Belirlenmesi

COSO KRY modelinin ikinci bileşeni risk yönetimi sürecinin ilk aşaması olan kurum amaçlarının belirlenmesidir;[93]

[91] COSO,ERM,a.g.e. s.9.
[92]Türkiye Etik Değerler Merkezi (Çevrimiçi: www.tedmer.org.tr, Erişim: 14.05.2012)

"Kurum amaçları stratejik amaçlar seviyesinde belirlenir ve operasyonel, raporlama ve mevzuata uyum amaçlarına bir temel teşkil ederler. Her kurum içsel ve dışsal nedenlerden kaynaklanan muhtelif risklerle karşılaşır ve risk tanımlama, değerlendirilmesi ve risklerin giderilmesi süreçlerinin etkin olabilmesinin temel koşulu kurum amaçlarının belirlenmesidir. Kurum amaçları risk toleransını etkileyen risk iştahına uyumlu olmalıdır."

Kurum amaçları aynı zamanda kurumun varlık ve faaliyette bulunma nedenleridir. Bir kurumun amaçlarının belirlenmesi stratejik hedeflerinin belirlenmesi ile başlar. Bunun ilk adımı da stratejik bir vizyonun oluşturulmasıdır. KRY amaçların belirlenmesi aşamasını şu adımlarla özetlemektedir;[94]

Misyon/Vizyon -»Ana Stratejik Hedefler -» Stratejiler-» İlgili amaçlar

Yukarıdaki şema kurumun misyonundan başlayarak kurumun en üst seviyeden en alt seviyeye kadar hedef belirleme sürecini özetlemektedir. Söz konusu süreçteki aşamaları şu şekilde açıklamak mümkündür;

Vizyon, muhtelif tanımları olmasına rağmen kısaca kurumun gelecekte ve uzun vade de gelmek istediği yer veya olmak istediği konum olarak özetlenebilir. Misyon ise, kurumun halihazırda yaptıkları, bulunduğu yer, servis ve ürünlerini veya becerilerini anlatan, kim, ne, neden ve nasıl gibi soruların çok kısa ve anlaşılır kelimelerle açıklanmaya çalışıldığı ifadelerdir. Vizyon ve misyon aynı zamanda sadece etkileyici veya gösterişli ifadeler olmayıp kurumun gerçekleştirmeye çalışacağı hedeflerin, ulaşmak istediği noktanın özet halini de ifade etmektedir. Bu nedenle vizyon ve misyonun belirlenmesinden sonra bunların nasıl gerçekleştirileceği ana stratejik hedeflerde ifade edilmektedir.

KRY modeli amaç bazlı bir modeldir. Temel çalışma sistemi olarak kurumun amaçlarını ve bu amaçlara yönelik riskleri esas alan bir yapısı vardır. Ancak, kurumlarda söz konusu hedefler iş süreçleri aracılığıyla gerçekleştirilmektedir. Hatta iş süreçleri birim yapılanmalarının temelini oluşturmaktadır. Örneğin, insan kaynakları iş süreçleri açısından bakıldığında işe alma, eğitim, tayin/terfi, ücret ve sosyal güvenlik işlemleri gibi alt süreçler kurumun büyüklüğüne göre farklı birimler altında organize

[93] COSO,ERM,a.g.e. s.13.
[94] Özbek, a.g.e. s.299.

edilmektedir. Bu nedenle, operasyonel, raporlama ve mevzuata uyum hedeflerinin mevcut iş süreçleri ile ilişkisinin kurulmasında fayda vardır.[95]

Bu ilişkinin nasıl kurulacağı beşinci bölümde bir uygulama örneği üzerinde anlatılmaya çalışılacaktır.

2.2.2.3.Olayların Tanımlanması

Kurumun hedeflerine ulaşmasını etkileyen, risk ve fırsatlar arasında değişen iç ve dış olaylar tanımlanır. Riski etkili bir biçimde yönetebilmek için önce varlığının fark edilmesi gerekmektedir. Bu görevde etkin olabilmek için kurum yönetimi, hem iç hem de dış kaynaklı çeşitli faktörleri göz önünde bulundurmak zorundadır.[96]

Olayların tanımlanması aşaması, bir önceki adımda belirlenen kurum amaçlarının gerçekleştirilmesini olumlu etkileyebilecek fırsatların veya olumsuz etkileyebilecek risklerin diğer bir deyişle kurumun hedeflerini gerçekleştirmesini olumlu veya olumsuz etkileyebilecek tüm "olay" ların tanımlanması aşamasıdır. Risk kavramı genel olarak belirsizliklerin olumsuz tarafını veya kurumun faaliyetlerini olumsuz etkileyebilecek tehditleri yansıtmaktadır. Diğer yandan, belirsizlikler kurumlar için olumsuz sonuçlar yaratabileceği gibi fırsatlarda yaratabilecektir. Bu aşamada "risk" yerine "olay" kelimesinin kullanılmasının nedeni belirsizliklerin yaratacağı hem risklerin hem de olası fırsatların tanımlanmasıdır. KRY modelinde olay tanımlaması adımı şu şekilde açıklanmaktadır;[97]

"*Yönetim, gerçekleşmesi halinde kurumu etkileyebilecek olası olayları tanımlar ve bu olayların bir fırsatı temsil edip etmediğini veya kurumun stratejilerim başarıyla hayata geçirmesi ve hedeflerini gerçekleştirmesini olumsuz etkileme ihtimalinin olup olmadığım belirler. Olumsuz etkiye sahip olaylar yönetim değerlendirmesini ve önlem alınmasını gerektiren riskleri temsil ederler. Olumlu etkiye sahip olaylar ise fırsatları temsil ederler ve yönetim bu fırsatları stratejik hedeflerin oluşturulmasında kullanır. Olayların tanımlanmasında yönetim riskler içerecek veya fırsatlar sunabilecek içsel ve dışsal faktörleri tüm kurumu kapsayacak şekilde dikkate alır."*

---

[95] COSO,ERM **''Integrated Framework''**,s.16.
[96] Işılda Arslan, **''Kurumsal Risk Yönetimi'',** Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Mart 2008,s.31.
[97] COSO, ERM a.g.e. s.18.

Tanımda yer alan "faktörler" ile daha önce bahsedildiği gibi gerek olumlu gerekse olumsuz etkiler yaratabilecek tüm gelişmeler kastedilmektedir. Diğer bir deyişle, faktörler geniş anlamlı unsurlar olup bu faktörlere bağlı riskler veya fırsatlar söz konusu olabilecektir.

COSO KRY modeli, belirsizlikleri hem olumlu hem de olumsuz açılardan değerlendirmeyi hedeflemektedir. Belirsizliklerin olumsuz yanları kurumun yönetmesi gereken riskleri, olumlu yanları ise kurum açısından değerlendirilebilecek fırsatları ifade etmektedir. Geçmişte risk yönetimi belirsizliklerin olumsuz yönlerine risklere ağırlık vermekteyken günümüzde fırsatlar da dikkat alınmakta, diğer bir deyişle, hem aşağı yönlü hem de yukarı yönlü riskler dikkate alınmaktadır. KRY de model olarak her iki yönlü risk ve fırsatlara vurgu yapmaktadır.[98]

COSO KRY modeli, risk sınıflandırmasını iki aşamada ve iki yönlü yapmaktadır. KRY olay tanımlanması aşamasında önce belirsizlik kaynağı, olabilecek ana faktörleri tanımlamakta sonrasında bu ana faktörlerin altında olası olayları "risk ve fırsatlara yol açabilecek olası gelişmeleri" açıklamaktadır. KRY' e göre iki ana belirsizlik kaynağı dışsal ve içsel faktörlerdir. Dışsal faktörler, kurumun faaliyette bulunduğu ekonomik, sosyal, yasal ortamdan kaynaklanan faktörleri ifade etmekte, içsel faktörler ise kurumun finansal yapısı, örgütsel yapılanması, insan kaynağı ve kullandığı teknolojiler gibi kendisinden kaynaklanan olayları ifade etmektedir.

Söz konusu içsel ve dışsal faktörlerin neden olabileceği olaylara ise aşağıdaki hususlar örnek olarak verilmektedir. KRY modelinde sunulan örneklere ülkemiz koşulları dikkate alınarak bazı ilaveler yapılmıştır.[99]

Dışsal Faktörler;

- Ekonomik faktörler
- Ulusal ekonomik gelişmeler; Enflasyon, işsizlik ve işgücü piyasası, dış ticaret, ekonomik büyüme, ekonomik istikrar, hammadde, enerji fiyat ve tedarik koşullarındaki gelişmeler,

[98] COSO, ERM a.g.e. s.19.
[99] Paul Sobel, **''Internal Auditing''**,2007.s.21.den aktaran , Özbek, s.319

Küresel ekonomik gelişmeler; Global ekonomik büyümedeki artış veya azalışlar, global ticaretteki gelişmeler, komşu ülkelerdeki ekonomik gelişmeler, olası bir global kriz, global likidite koşulları, global yatırım ortamındaki değişimler,

- Pazarın geleceğine ilişkin beklentiler; pazarın mevcut büyüklüğü, büyüklük veya gelişme hızındaki değişimler, pazarın yapısındaki değişimler,

İçsel Faktörler;

- Kurum altyapısından kaynaklanan faktörler
- Hataların azaltılmasını engellemek amacıyla altyapı yatırımlarına yatırım yapılma ihtiyacı, çağrı merkezi yatırımı, yenileme yatırımları vb.
- insan kaynakları
- Olası işyeri kazaları, artniyetli personel eylemleri, grev olasılığı,
- İnsan kaynağının uzmanlığı ve teknik yeterliliği,
- Nitelikli insan kaynağı ve anahtar yöneticilerin değişimleri,
- Yeniliklere açık olma, yönetsel değişimlerin kabul edilebilme gücü.

Risklerin tanımlanması aşamasında yapılması gereken husus, kurumun bir önceki adımda açıklanan stratejik, operasyonel, raporlama ve mevzuata uyum konularındaki tüm hedefleri olumsuz etkileyebilecek olası risklerin bir listesinin veya bir envanterinin çıkarılmasıdır. KRY modeli söz konusu risk envanterinin çıkarılmasında hangi metodolojilerin kullanılabileceğine dair açıklayıcı önerilerde bulunmaktadır. Aşağıda belirtilen tüm metodolojiler COSO' nun KRY modelinden alınmış ancak daha iyi anlaşılması amacıyla bazı ilave açıklamalar yapılmıştır. Söz konusu metodolojiler şu şekilde olabilir;[100]

Olay envanterleri; Olay envanterleri, gerek içsel gerekse dışsal kaynaklardan faydalanarak olası bir risk envanterinin çıkarılmasıdır. Örneğin, yukarıda örnekleri verilen ve birer ticari ürün olan risk sınıflandırma modelleri incelenerek olası bir risk envanteri çıkarılabileceği gibi faaliyette bulunulan sektörde yaşanan problemlerin basındaki haberler veya internet yoluyla taranarak olası risklerin tespitine çalışılabilir. Örneğin, yeni bir üretim hattının planlanmasında sektörde daha önce benzer deneyime sahip kurumların yaşadıkları sorunların analiz edilmesi, yeni bir dağıtım kanalının

[100] COSO, **Enterprise Risk Management. ,Executive Summary Integrated Framework**, Application Techniques,2004, (Çevrimiçi: www.coso.org, Erisim: 27.12.2012)s.21.

geliştirilmesinde yine sektörde daha önce yaşanan aksaklıkların analiz edilmesi olası risklerin tanımlanmasına yardımcı olacaktır. Bu çalışma, risk yönetimi proje grubu tarafından yapılabileceği gibi tamamen ayrı bir grup tarafından veya bu konularda tecrübeli olduğu düşünülen kurum çalışanlarından oluşturulan bir grup tarafından da yapılabilir.[101]

Arama grup çalışmaları veya arama konferansları; Kurum içerisinde muhtelif bölümlerden çalışanların katılımıyla gerçekleştirilen arama konferansları veya grup çalışmaları yoluyla risk envanteri çıkarılabilir. Arama konferansları ülkemizde son yıllarda giderek yaygınlaşan bir çalışmadır. Genellikle, tüm kademelerden kurum yönetici ve çalışanlarının hafta sonu bir merkezde veya otelde toplanarak bir moderatör eşliğinde iki gün veya daha uzun süren tartışma ve görüş alışverişinde bulunması yoluyla yapılan çalışmalardır.[102]

2.2.2.4.Risklerin Değerlendirilmesi

Bir önceki aşamada kurumların karşılaşabileceği tüm riskler belirlenerek bu çalışmanın nasıl yapılacağı konusu üzerine risk envanteri çıkarılması üzerinde durulmuştu. Riskler tanımlandıktan sonra bunların kurum üzerindeki olası etkilerinin ve meydana gelme olasılıklarının değerlendirilmesi gerekir.[103]

COSO KRY modeli risklerin değerlendirilmesi aşamasını şu şekilde özetlemektedir;[104]

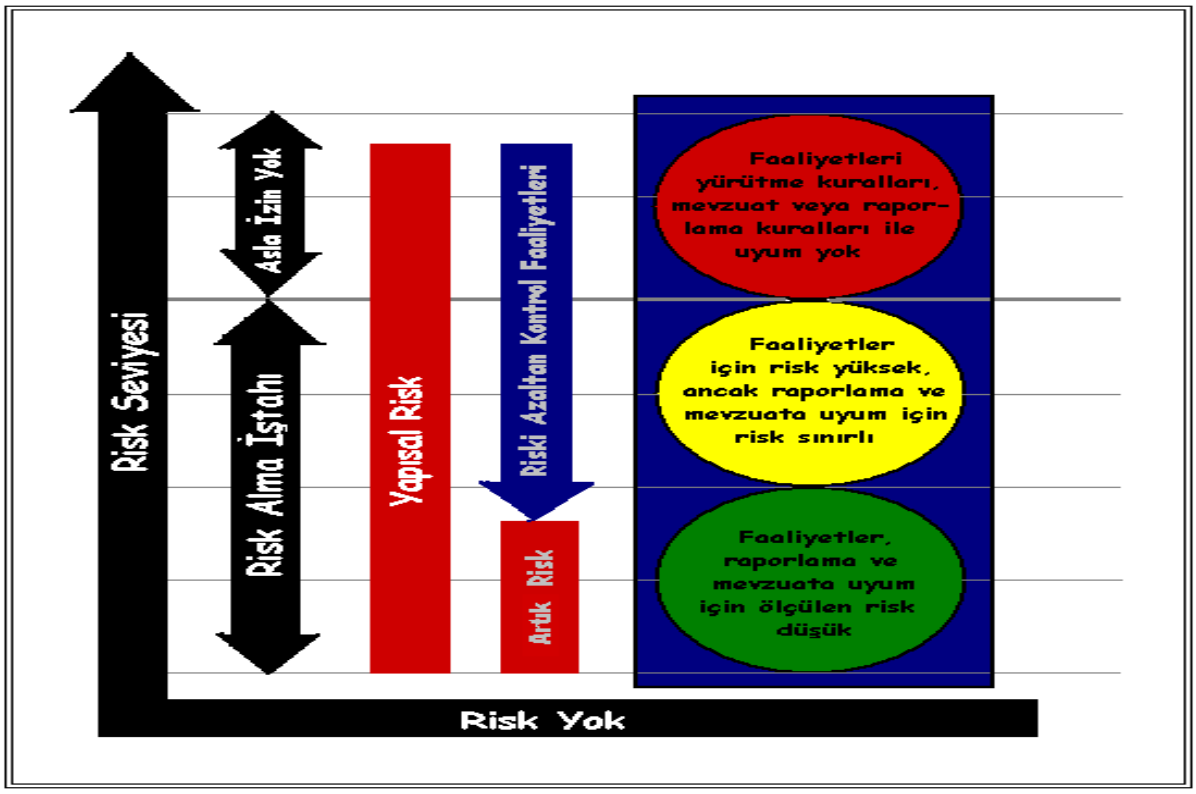
"Risk değerlendirmesi, bir kuruma, hedeflerinin gerçekleştirilmesi üzerinde hangi olası olayların ne ölçüde etkili olacağını göz önünde bulundurmaları konusunda yardımcı olur. Yönetim olayları gerçekleşme olasılığı ve etkilerini göz önünde bulundurarak değerlendirir ve normalde sayısal ve sayısal olmayan değerlendirme yöntemlerinin bir bileşenini kullanır. Olası olayların olumlu ve olumsuz yanları her bir risk bazında veya kategori veya risk sınıfı bazında ve tüm kurum çapında değerlendirilmelidir. Riskler gerek doğal veya içsel riskler ve gerekse kalıntı riskler temel alınarak değerlendirilir."

[101] COSO, ERM a.g.e. s.24.
[102] COSO, ERM a.g.e. s.31.
[103] Arslan, a.g.e. s.33.
[104] COSO, ERM a.g.e. s.34.

Risk değerlendirmesi yaparken aşağıda sıralanan kavramları açıklamak konuyu kavrama açısından daha etkili olacaktır.

İçsel Risk, Artık Risk

Riskin iki temel bileşeni söz konusudur. İlki doğal risk; işlem süreçlerinin doğasında varolan içsel, doğal risk seviyesidir. Her işlem sürecinin doğası gereği az veya çok mutlaka bir risk unsuru içermesi söz konusudur. İkincisi ise "artık" önlenemeyen risk; her işlem sürecinde mevcut iç kontrol uygulamaları ile kontrol altına alınmaya çalışılan risklerden başka "artık" risk olarak tanımlanan bir bölüm risk geriye kalmaktadır. Risklerin uygun iç kontrol yöntemleriyle minimize edilmesi planlanmaktadır.[105]



Şekil 5- İçsel- Artık Risk

(Kaynak: Agency Risk Management and Internal Control Standards / Appendix A: Implementation Tools,2005, Virginia)

Doğal veya içsel risk, herhangi bir sürecin doğasında yer alan ve bu riskin giderilmesi için herhangi bir kontrol faaliyetinin geliştirilmemesi halinde meydana

[105] Keskin Duygu Anıl, **''İç Kontrol Sistemi Kontrol öz Değerlendirme'',** Beta yayınevi, İstanbul, 2006, s. 16

gelecek zararı ifade etmektedir. Artık risk ise, söz konusu doğal riske yönelik mevcut kontrol önlemleri uygulanmasına rağmen kontrol edilemeyen ve riskin gerçekleşmesi halinde uygulanmakta olan kontrol önlemlerine rağmen oluşma ihtimali olan riski ifade etmektedir. KRY bu konuyu şu şekilde açıklamaktadır.[106]

" İçsel risk söz konusu riskin gerçekleşme olasılığı veya etkisinin değiştirilmesi yönünde herhangi bir yönetsel faaliyetin olmadığı bir durumdaki risktir. Kalıntı risk ise yönetimin söz konusu riske yönelik önleminden sonra kalan risk seviyesidir."

Risklerin yönetilmesi için alınan kontrol önlemleri söz konusu risklerin gerçekleşme olasılığını azaltabileceği gibi yaratacağı olumsuz etkilerinde azaltılmasını sağlayabilirler veya bir risk için hem gerçekleşme olasılığını azaltıcı hem de yaratacağı etkiyi azaltıcı ayrı ayrı kontrol önlemleri alınabilir. Sonuçta alınan bu tek veya birden fazla önlemin amacı söz konusu riskin gerçekleşmesi halinde yaratacağı hasarın en aza indirilmesidir.[107]

Olasılık - Etki Analizi

Risk yönetiminde üzerinde mutabık kalınan bir değerleme yöntemi risklerin gerçekleşme olasılıkları ve yaratacakları etkiler dikkate alınarak değerlendirilmesidir.[108]

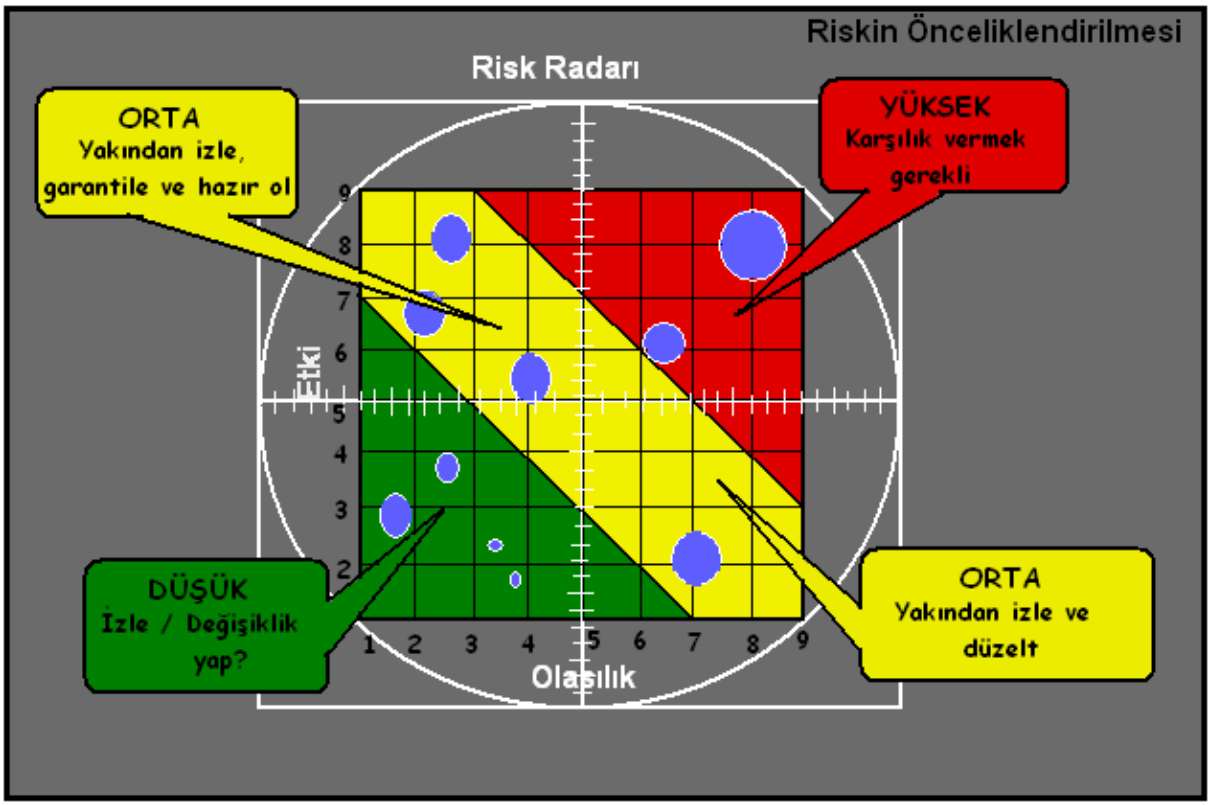
Risklerin gerçekleşme olasılığı hangi sıklıkla gerçekleşeceğinin veya hangi yüzdeyle gerçekleşeceğinin tahmin edilmeye çalışılmasıdır. Gerçekleşme olasılığı her risk için aynı olmadığı gibi sıklıkla kastedilen zaman süresi de her risk için eşit değildir.[109]

Değerlendirmenin ikinci boyutu ise, söz konusu riskin gerçekleşmesi halinde yaratacağı zararın boyutunun tahmin edilmesidir. Aynı şekilde, her riskin yaratacağı etki de birbirine eşit değildir. Bazı risklerin yaratacağı olumsuz etki göz ardı

[106] COSO, ERM a.g.e. s.39.
[107] David Griffiths, **"Risk Based Internal Auditing –Three Vıews On Implemantation"** , 15 March 2006,(Çevrimiçi:http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf , Erişim:03.03.2012),s.1
[108] Süleyman Uyar, ''**İç Kontrol ve İç Denetim 5018 sayılı Kanun Açısından Değerlendirme,''** Gazi Kitapevi, Ankara, 2009, s.40.
[109] Uyar, a.g.e. s.42.

edilebileceği gibi bazı riskler kurumun varlığını dahi tehlikeye atacak şiddette zarara neden olabilirler.[110]

Risklerin gerçekleşme olasılığı ile yaratacağı etkiler arasında doğrudan bir ilişki olması zorunluluğu olmamakla birlikte; riskler gerçekleşme olasılıkları ve yaratacakları hasarın bir arada değerlendirilerek risklerin gösterildiği şekle aşağıda yer verilmiştir.



Şekil 6-Risklerin Önceliklendirilmesi

Kaynak: (Çevrimiçi:http://www.kier.kyotou.ac.jp/fetokyo/symposium/sympo2007/shenkir.pdf)

Risklerin gerçekleşme olasılığı ve yaratacağı etkinin tahmin edilmesinde hem sayısal hem de sayısal olmayan ölçüm teknikleri kullanılabilmektedir. KRY bu konuyu şu şekilde açıklamaktadır;[111]

"Bir kurumun risk değerlendirme metodolojisi sayısal ve sayısal olmayan tekniklerin bileşiminden oluşur. Yönetim, risklerin sayısallaştırılmasının mümkün olmadığı, riski sayısallaştırmak için güvenilir verilerin veya söz konusu veriyi elde etmenin maliyet açısından çok anlamlı olmadığı durumlarda sayısal olmayan teknikleri

[110] COSO, ERM a.g.e. s.43.
[111] COSO, ERM a.g.e. s.45.

kullanabilir. Sayısal teknikler daha kesin bir kanaat verirler ve sayısal olmayan teknikleri desteklemek için daha karmaşık faaliyetler kullanılır."

KRY modeli risklerin gerçekleşme sıklığı ve olası etkilerinin değerlendirilmesinde içsel veya doğal riskler için bazı temel ölçüm yöntemleri önermektedir. Bunlar sırasıyla nominal ölçüm, sıralama ölçümü, aralıklı ölçüm, oran ölçümlemesi' dir.

Bu yöntemler sırasıyla aşağıda açıklanmıştır.[112]

Nominal ölçümleme; *Risklerin (olayların) ekonomik, teknolojik ve doğal ortam gibi gruplara ayrılmasıdır. Risklerin sınıflandırılmasına da benzeyen bu uygulamada herhangi bir önceliktendirme, önem sırasına koyma söz konusu olmamaktadır. Risklere tahsis edilen numaralar sadece tanımlama amacını gütmekte olup bu numaraların sıraya konulması mümkün değildir.*

Sıralama ölçümü; *Burada riskler bir önem sırasında konulmaktadır. Burada sıralama yüksek, orta veya düşük gibi kategorilere ayrılabilmekte veya 1 den başlayarak 3 veya 5 basamaklı bir önem sıralaması yapılmakta ve riskler önem derecesine göre bu derecelerden birisine dahil edilmektedir.*

Aralıklı ölçüm; *Aralıklı ölçüm birbirine eşit mesafedeki aralıklardan oluşan bir sıralama yöntemidir. Örneğin, önemli bir makinedeki üretim kaybının değeri "3", bir saatlik bir elektrik kesintisinin yol açacağı zarar* "6", *ve 100 kişilik eksik istihdamın etkisinin ise* "9" *olduğunu varsayarsak, yönetim önemli bir makinedeki üretim kaybı ve bir saatlik enerji kesintisinin olası etkilerinin 100 kişilik eksik istihdamın yol açacağı etkiyle aynı olduğunu düşünebilecektir.*

Oran ölçümlemesi; *Oran ölçümlemesi,bir olayın etkisinin "3 " diğer bir olayın etkisinin* "6" *olarak değerlendirilmesi halinde ikinci olayın birinci olaya oranla iki kat etkiye sahip olduğunun düşünülmesine imkan vermektedir.*

Yukarıda açıklanmaya çalışılan risk ölçümleme yöntemlerinden nominal ölçümleme ve sıralama ölçümlemesi sayısal olmayan, aralıklı ölçümleme ve oran ölçümlemesi ise sayısal ölçümleme yöntemleridir.

[112] COSO, ERM a.g.e. s.46.

Sayısal Olmayan Risk Ölçümleme Yöntemleri

Finansal veya sayısal rakamlara dökülebilen risklerin ölçümünde sayısal ölçüm tekniklerinin daha doğru bir sonuç vereceği kesindir. Ancak, kurumun amaçlarını gerçekleştirmesini engelleyebilecek risklerin tamamının sayısallaştırılabilmesi ve etkilerinin rakamsal olarak ölçülmesi veya tahmin edilmesi birçok durumda mümkün olmayacaktır. Bu durumda, olası risklerin olasılık ve etkilerinin değerlendirilebilmesi için sayısal olmayan ölçüm yöntemlerine başvurmak gerekecektir.[113]

Sayısallaştırılmayan risklerin gerek gerçekleşme olasılığı gerekse yaratacakları etkilerin ölçülmesinde en yaygın yöntem "derecelendirme" sistemidir. Derecelendirme sisteminde en düşükten en yükseğe kademeli olarak artan bir derecelendirme yapılmaktadır. Gerçekleşme olasılığı veya etkisi en düşük olan risklere 1 den başlayarak derece veya puan verilmekte, göreceli olarak gerçekleşme olasılığı veya etkisi daha yüksek olan risklere 2 puan verilmekte ve bu şekilde olasılığı en yüksek risklere doğru en yüksek puan olarak 5 veya 7 puana kadar bir derecelendirme yapılmaktadır. Bazı uygulamalarda az, orta ve yüksek olarak sadece 1, 2 ve 3 puandan oluşan bir derecelendirme yapılmakla birlikte; en kolay uygulama 5 üstünden yapılan bir değerlendirmedir.[114]

Gerçekleşme olasılığını gösteren bir derecelendirme de puanlar ve anlamları Beşinci bölüm uygulama örneğinde verilmiştir.

Sayısal Risk Ölçümleme Yöntemleri

Sayısal risk ölçümleme yöntemleri olasılık, olasılık dışı ve karşılaştırma tekniklerinden oluşmaktadır.[115]

Olasılık teknikleri ; *Olasılık temelli teknikler, risklerin gerçekleşme olasılığı ve etkilerini söz konusu risklerin davranışlarının dağılımı varsayımına dayalı olarak ölçmektedir. Riske maruz değer, riske maruz nakit akımı, riske maruz gelir gibi riske maruz olma tekniklerinin yanı sıra kayıplara yol açan olayların değerlendirilmesi ve geriye dönük testler gibi tekniklerde içermektedir. Aşağıda temel tanımlara yer verilmekle birlikte; detaylara girilmemiştir.*

[113] Çetin Özbek, **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol,** TİDE Yayınları İstanbul, Ekim 2012, s 350.
[114] Deloitte,**'' İç Denetim Hizmetleri''**, Kurumsal Risk Hizmetleri Yayın Broşürü ,s.49.
[115] COSO, ERM a.g.e. s.48.

Riske maruz değer; *Riske maruz değer, istatistiki olarak belirli bir güven aralığında (genellikle % 95) belirli bir zaman periyodunda bir aktifin değerinde meydana gelebilecek en yüksek kaybı ifade etmektedir.*

Geriye dönük testler; *Back testing bir stratejinin, bir hipotezin veya bir varsayımın geriye dönük tarihsel veriler üzerinden test edilmesidir.*

Duyarlılık Analizi; *Herhangi bir istatistiki modelde para- nn'jri'lrrdeki değişikliklerin modelin çıktısına nasıl etki edeceğini incelemektedir.*

Senaryo analizi; *Herhangi bir projeksiyonda muhtemel sonuçlara göre çıktıların hesaplanmasıdır. Örneğin, satış projeksiyonlarında ekonomik büyümenin hızlı orta hızlı ve yavaş olmasına göre satış projeksiyonları yapılması bir örnektir.*

Stres testi: *Herhangi bir aktifte veya portföyde olası değişikliklerin portföyü veya göz konusu aktifi ne ölçüde etkileyeceğini tahmin etmeye yarayan metottur. Avrupa bankaların kredi portföylerinin faiz oranlarındaki değişikliklere karşı ne ölçüde kırılgan olduğunun test edilmesi buna bir örnektir.*

Karşılaştırma teknikleri; *Karşılaştırma teknikleri özellikle risklerin gerçekleşme olasılığı ve etkilerinin tahmin edilmesinde gerek kurumun kentli içindeki tecrübeler gerekse rakiplerin ve sektördeki diğer kurumların tecrübelerinden faydalanma amacını gütmektedir.*

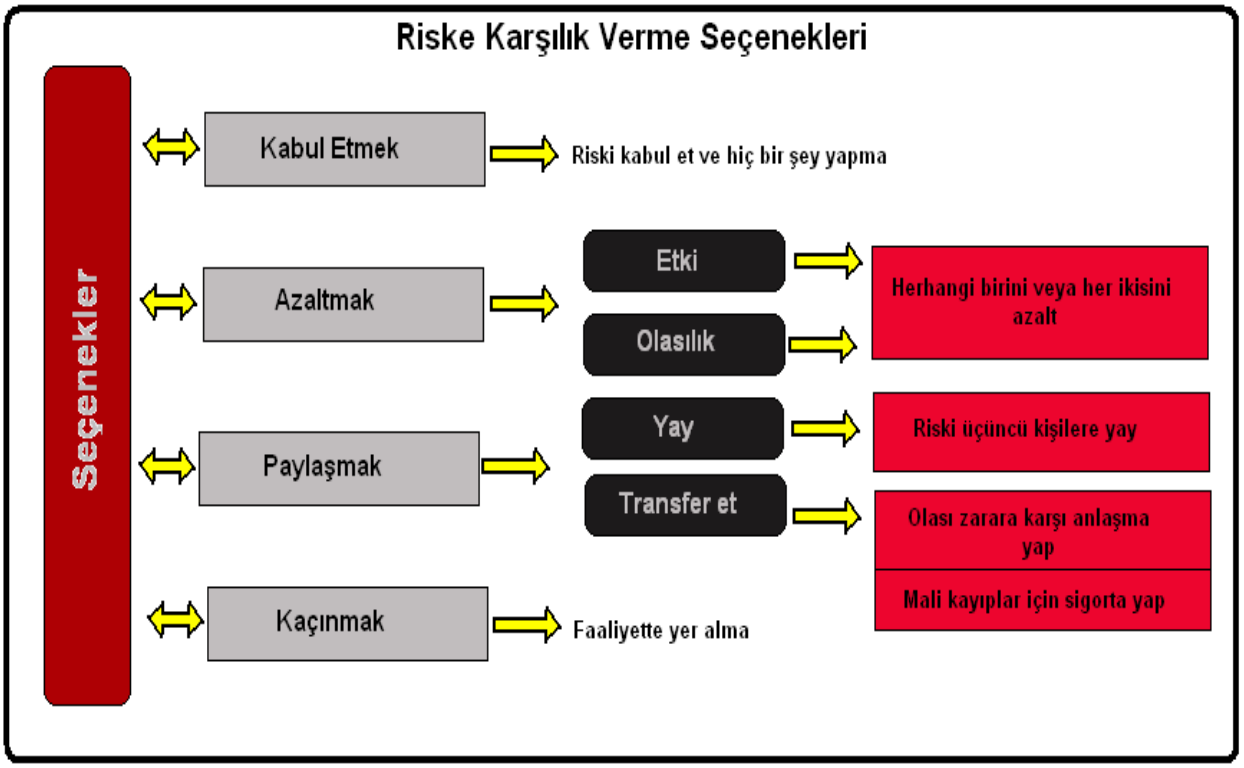
Risklerin Biraraya Getirilmesi

Risklerin gerek sayısal gerekse sayısal olmayan yöntemlerle etki ve gerçekleşme olasılıklarının değerlendirilmesinden sonra yapılması gereken, bütün risklerin bir araya getirilmesidir. Bir araya getirilen riskler en yüksek gerçekleşme olasılığı ve en yüksek etki açısından bir sıralamaya tabi tutularak hangi risklerin en yüksek gerçekleşme olasılığı ve etkiye sahip olduğu, dolayısıyla öncelikle giderilmesi gereken risklerin neler olduğuna dair bir öncelikli riskler listesine sahip olunacaktır.[116]

[116] Paul Sobel, **''Internal Auditing''**,2007.s.16. dan aktaran, Özbek, s.362.

2.2.2.5. Risklere Karşılık Verme

Risklerin giderilmesi, gerçekte risklere verilecek tepkiyi, alınacak önlem ve aksiyonları, diğer bir deyişle, söz konusu risklerin giderilmesi veya azaltılması çalışmalarının tümünü kapsamaktadır.



Şekil 7- Riske Karşılık Verme Seçenekleri

Kaynak: (Çevrimiçi:http://www.hm-treasury.gov.uk./media/5/D/Green_Book_07.pdf)

COSO KRY modeli tarafından önerilen ve genel kabul görmüş dört risk giderme yöntemi vardır. Bunlar sırasıyla riskten kaçınma, riski azaltma, riski paylaşma ve riski kabul etmektir.[117]

Riskten kaçınma; *Riskleri kabul etmektense riskli süreci hiç gerçekleştirmeme veya hiçbir şekilde o riski kabul etmemektir, örneğin deprem riskinin yüksek olduğu bir alanda nükleer enerji tesisi yapılmaktan kaçınılması en bariz örnektir.*

Risklerin azaltılması; *Muhtelif kontrol önlemleriyle olası risklerin etkilerinin azaltılmaya çalışılmasıdır. Ürün sayısının çeşitlendirilmesi, operasyonel limitler belirlenmesi işlem süreçlerinin etkinleştirilmesi, karar alma süreçlerine yönetimin daha*

[117] COSO, ERM a.g.e. s.55.

fazla dahil olması, üst düzey yöneticilerin faaliyetleri izlemesinin etkinleştirilmesi, finansal risklerin yönetimi amacıyla portföy yatırımlarında çeşitliliğe gidilmesi, operasyonel birimler arasında sermayenin yeniden dağıtılması olası risklerin azaltılması çabalarına örnektir.

Risklerin paylaşılması; *Olası risklerin etkilerinin başka taraflarla paylaşılmaya çalışılmasıdır. Beklenmeyen zararlara karşı sigorta ürünlerinin kullanılması, riskin tamamını üstlenmemek amacıyla ortaklıklara girilmesi, sendikasyon anlaşmalarına gidilmesi, sermaye piyasası araçları aracılığı ile risklerin hedge edilmesi, belli iş süreçlerinin outsource edilmesi, müşteriler, tedarikçiler, ve diğer iş ortaklarıyla kontratlar yoluyla risklerin paylaşılması bu çabalara örnek olarak verilebilir.*

Risklerin kabul edilmesi; *Söz konusu riskin varlığına rağmen üstlenilerek kurumun kendi imkanlarıyla olası riskler için karşılık ayırması, riskin kurumun risk iştahı içinde kalması kaydıyla önlem alınmadan süreçlerin işletilmeye devam edilmesidir. Diğer bir deyişle, söz konusu riske rağmen riskin sonuçlarına katlanılma kararı verilerek faaliyetlere devam edilmesidir.*

2.2.2.6.Kontrol Faaliyetleri

Risklere verilecek karşılıklar belirlendikten sonra, riskleri minimize etmek için yöntemler geliştirme safhasına geçilir.

Bunun yanında politika ve prosedürler, diğer kurum talimatlarının da yerine getirilmesini sağlamaya yöneliktir. Tüm kurumda, her seviyede ve tüm fonksiyonlarda geçerlidir. Onaylar, izinler, soruşturmalar, anlaşmalar, performans gözden geçirmeleri, güvenlik ölçütleri ve uygun belgelerin oluşturulması ve muhafazası gibi geniş bir yelpazedeki faaliyetleri içerir. Kısacası bu faaliyetler temel kurum uygulamalarıdır.[118]

Kontrol faaliyetleri; yönetimin talimatlarının yerine getirilmesini sağlamaya yarayan politika, prosedür ve süreçlerdir.[119] Onaylar, yetkilendirmeler, öneriler,

[118] Arslan, a.g.e, s.38.

[119] E.Paul Lındow, ve D. Race Jill, Beyond Traditional Audit Techniques, ‘’**Journal of Accountacy Issues’’**, July 2002, s.9.

performans incelemeleri, varlıkların güvenliği ve görevlerin ayrılığı gibi faaliyetleri içermektedir.[120]

COSO- KRY modeli kontrol faaliyetlerini şu şekilde özetlemektedir;[121]

"Kontrol faaliyetleri, yönetim tarafından risklerin giderilmesine yardımcı olan politika ve prosedürlerdir. Kontrol bütün organizasyon boyunca bütün yönetsel kademelerde ve bütün fonksiyonları kapsayacak şekilde gerçekleştirilir. Kontrol faaliyetleri onaylama, yetkilendirme, mutabakat, operasyonel performansın gözden geçirilmesi, aktiflerin muhafazası ve görevlerin ayrılığı ilkesini de içeren oldukça geniş bir faaliyet dizisini kapsar."

Bir riskin oluşması, çoğu durumda kurumun kendisi dışında oluşabilecek bir durumken kontrol faaliyeti söz konusu risklere yönelik kurum yöneticilerinin kendi iradeleriyle aldıkları önlemleri ifade etmektedir. Diğer bir deyişle, riskin oluşumunda kurumun doğrudan herhangi bir etkisi söz konusu olmadığı halde, kontrol faaliyetlerinin oluşturulması ve işletilmesinde kurum yöneticilerinin tam bir hakimiyeti söz konusudur.

Alınacak önlemler konusunda vurgulanması gereken bir diğer husus, risklere yönelik alınacak önlemlerin büyük ölçüde işlem süreçlerine yönelik kontrol önlemlerinden oluşacaktır.

Kontrol önleminin geliştirilmesi iç kontrol konusunda detaylı bir bilgi birikimine gereksinim gösterecektir. Normal koşullar altında kurumun iç denetim birimi denetçilerinin bu bilgilere uzmanlık seviyesinde sahip olmaları beklenmelidir.

Uygun kontrol önlemlerinin seçimi ve uygulamaya konulması aşamasından sonra kurumun artık asgari seviyede bir risk yönetimi sistemine sahip olduğunu düşünülebilir. Bu aşamadan sonra yapılması gereken sistemin işlerliğinin sağlanmasıdır. Bu ise, işleyişe ilişkin her türlü bilginin üretilmesi, ilgili kademelere raporlanmasının yanı sıra söz konusu risklerde meydana gelen değişikliklerin ve bu risklere yönelik kontrol önlemlerinin ilgili riskleri önleme veya gidermedeki yeterliliklerinin periyodik olarak değerlendirilmesini gerektirecektir.[122]

---

[120] Robert Moeller, ‘’**Brink’s Modern Internal Auditing’’,** Sixth Edition, New Jersey, John Wiley&Sons, 2005, s.94.
[121] COSO, ERM a.g.e. s.63.
[122] COSO, ERM a.g.e. s.64.

Kısacası bu faaliyetler temel kurum uygulamalarıdır. Burada yöneticilerin dikkat etmesi gereken şey riskleri en aza indirmek için yapılan bu kontrol faaliyetlerinin aşırıya kaçması en az aşırı risk kadar tehlikeli olduğudur.

2.2.2.7.Bilgi ve İletişim

Kişilerin sorumluluklarını yerine getirmesi için ilgili bilgi belli bir biçimde ve belli zaman aralıkları ile tanımlanır, ele geçirilir ve iletilir. Kurumsal risk yönetimi gibi bir güç, riskin etkili olarak değerlendirilmesi ve yönetilmesi için zaruri olan, zengin miktarda veri kümesine ihtiyaç duyar. En uygun durumda, bu bilgi tanımlanan riskleri yönetmek, analiz etmek ve izlemekle sorumlu kişiler tarafından kullanılmak üzere uzmanlaşmış bir sistem ve/veya veri tabanında depolanır. Bu veriler, yönetim kurulu ve idarecileri de kapsayan kurumun her seviyesindeki iletişime temel oluşturur.[123]

KRY Modeli bilgi ve iletişim adımını şu şekilde açıklamaktadır;[124]

"İlgili bilgi, tanımlanmalı, elde edilerek kullanılmalı, çalışanların sorumluluklarını yerine getirmelerini sağlayacak bir şekil ve zaman çerçevesinde iletilmelidir. Bilişim teknolojileri gerek içsel kaynakları gerekse kurum dışındaki bilgi kaynaklarını kullanarak risklerin yönetilmesi ve kurum hedeflerine ilişkin bilgili karar alınması için gerekli bilgiyi sağlarlar. Etkili iletişim aynı zamanda yukarıdan aşağıya, aşağıdan yukarıya ve bütün kurum boyunca gerçekleşir. Bütün çalışanlar, kurumsal risk yönetimi sorumluluklarının ciddiye alındığına dair üst yönetimden net bir mesaj almalıdır. Herkes kurumsal risk yönetimindeki rol ve sorumluluklarının yanı sıra kendi faaliyetlerinin diğer çalışanların faaliyetleriyle olan ilişkisini de anlamalıdır. Tüm çalışanların kurum açısından önem taşıyan bilginin nasıl iletileceğine dair bir sistemi olmalıdır. Bunlara ilave olarak müşteriler, tedarikçiler, düzenleyici otoriteler ve diğer paydaşlar gibi kurum dışındaki taraflar ile de etkin bir iletişim kurulur."

Gerek dış kaynaklardan gerekse içsel olarak üretilen bilgi, strateji ve hedeflerin oluşturulması, risklerin tanımlanması, analiz edilmesi, nasıl giderileceklerinin kararlaştırılması için elde edilmekte ve analiz edilmekte, diğer yandan KRY sürecini etkilemekte ve diğer yönetsel faaliyetlerin yerine getirilmesinde kullanılmaktadır.[125]

---

[123] Arslan, a.g.e, s.39.
[124] COSO, ERM a.g.e. s.67.
[125] COSO, ERM a.g.e. s.67.

KRY, kurumların kurum içerisinde üretilen her türlü bilginin yönetilmesi için kuracakları yönetsel bilgi sistemlerinin mimarisinin ve kurulumunun kurumsal stratejinin önemli bir parçası olduğunu ve seçilen teknolojinin kurum hedeflerinin gerçekleştirilmesi için kritik öneme sahip olduğunu ifade etmektedir. Bazı kurumların bilgileri entegre sistemlerle yönetilmekte bazılarının bilgileri ise birim bazında ayrı ayrı yönetilmekte, risk yönetimi bilgiye olan ihtiyacı çok büyük ölçüde artırmakta, web tabanlı bilgi yönetimi stratejileri bilginin eşanlı olarak edinilmesini, saklanmasını, birim veya fonksiyonlara göre dağıtılmasını, muhtelif kaynaklardan gelen bilgilerin kontrolünü, verilerin manuel işlenmesinin minimize edilmesini kolaylaştırmaktadır.

İletişim; Kurum içerisinde elde edilen veya üretilen her türlü bilginin gerekli bütün kademelerle uygun yöntemlerle paylaşılmasıdır. İletişim, sadece bilginin iletilmesini değil tüm yönetsel kademeler arasında sağlıklı bir iletişimin ve karşılıklı anlayış ortamının oluşmasını da gerektirir.

"Yönetim özel bir şekilde çalışanlara kendi sorumluluklarını ve kendilerinden beklenen davranışları işaret eden bir iletişim ve yönlendirme sağlamalıdır. "[126]

KRY modeli, iletişim kanalları arasında, e-mail, sesli mesajlar, kurumsal bültenler, spesifik risk konularını destekleyen özel veritabanları, CEO'dan mektuplar, e-mail tartışma grupları, çalışanların kolay erişebileceği KRY ile ilgili bilgi içeren internet siteleri, kurumsal iletişim içerisine yedirilmiş mesajlar, organizasyon, fonksiyon veya lokasyon çapında webcast veya telekonferanslar, KRY'in anahtar konularını açıklayan veya kuvvetlendiren posterler, afişler, KRY konusunda sorumluluk taşıyan bir dizi fonksiyon veya birimlerden diğer çalışanlarla yüz yüze yapılan toplantıları saymaktadır.[127]

2.2.2.8.Gözlemleme

İşletmenin ulaşmaya çalıştığı hedefler ile onlara ulaşmak için gerekli olanları temsil eden unsurlar arasında doğrudan ilişki vardır. COSO küpü bu ilişkiyi göstermek üzere tasarlanmıştır. Bir kurumda kurumsal risk yönetiminin etkin işleyip işlemediğine karar vermek, bu sekiz unsurun bulunup bulunmadığı, bulunuyor ise etkin işleyip

[126] COSO, ERM a.g.e. s.79.
[127] COSO, ERM a.g.e. s.81.

işlemediğinin değerlendirilmesi sonucu ulaşılacak bir yargıdır. Dahası bu unsurlar etkili bir kurumsal risk yönetiminin kriterleridir.[128]

KRY'in son adımı tüm KRY sürecinin izlenmesini oluşturmaktadır. Bu izleme kurumun içsel ortamının risk yönetimi faaliyetlerinin uygunluğu için gözlenmesinden risklerin tanımlanması, değerlendirilmesi ve giderilmesi, kurum içerisinde gerekli doğru bilginin üretilmesi ve uygun kademelere iletilmesi süreçlerini de kapsayacak şekilde risk yönetiminin tüm aşamalarının izlenmesini kapsamaktadır.

"KRY sistemi, varlığı, ve bileşenlerinin zaman içerisindeki çalışması gözlenmelidir. Bu sürekli gözetim faaliyetleri, ayrı değerlendirmeler veya her ikisinin bileşimiyle yapılır. Sürekli gözetim yönetsel faaliyetlerin gerçekleştirilmesi sırasında yapılır. Ayrı değerlendirmelerin kapsam ve sıklığı risklerin değerlendirilmesine ve sürekli gözetim uygulamalarının etkinliğine bağlıdır. KRY sisteminin işleyişine ilişkin yetersizlikler yukarıya doğru raporlanmalı, önemli eksiklikler ise üst yönetim ve yönetim kuruluna raporlanmalıdır."[129]

Gözetim faaliyetleri; sürekli gözetim faaliyetleri ve ayrı gözetim faaliyetleri olarak iki şekilde gerçekleştirilebilmektedir. Sürekli gözetim, yönetimin günlük icrai faaliyetlerinin gerçekleştirilmesi sırasındaki uygulamalardan oluşmaktadır.

Ayrı değerlendirmeler ise risk yönetimi sistemlerinin etkinliği konusunda periyodik olarak yapılan değerlendirmeleri içermektedir. Bu ayrı değerlendirmeler, yöneticilerin kendisi, iç denetçiler, kurum dışından uzmanlar veya tüm bu unsurların bileşimi aracılığıyla da yapılabilir.

Risk yönetimi sisteminin etkili bir şekilde çalışması için yukarıdaki değerlendirmelerde saptanan tüm aksaklıkların ilgili üst düzey yöneticilere zaman geçirmeksizin raporlanması ve tespit edilen aksaklıklara yönelik ne tür iyileştirme önlemlerinin alınacağının tartışılması, kararlaştırılması ve uygulama sorumlularının belirlenmesi, ilerleyen aşamada da alman önlemlerin etkinliğinin değerlendirilmesi gereklidir.

[128] Arslan, a.g.e, s.39.
[129] COSO, ERM a.g.e. s.85.

BÖLÜM III

YENİ TÜRKTİCARET KANUNU KAPSAMINDA ANONİM ŞİRKETLERİN YAPISAL ÖZELLİKLERİ VE RİSK YÖNETİMİ'NİN ETKİLİLİĞİNİ DEĞERLENDİRME SÜRECİ

3.1. 6102 Sayılı Yeni Türk Ticaret Kanununun Anonim Şirketlere Getirdikleri Yenilikler

Giderek karmaşıklaşan iş dünyası, gelişen teknoloji ve artan ekonomik ilişkiler ve rekabet ve aynı paralelde getirilen yasal düzenlemeler işletmelerin karşılaştığı risklerin niteliğini ve boyutunu önemli ölçüde etkilemekte işletmelerde erken uyarı sistemlerinin daha biçimsel ve daha fonksiyonel şekilde kurulması ve işletilmesini gerekli kılmaktadır. Ülkemizde sürdürülebilir işletme olmanın hukuki temelini teşkil eden Anonim Şirketlere yasal mevzuatımıza diğer şirketlere oranla biraz daha fazla önem verilmekte ve bu türdeki şirketleşmeler biraz daha teşvik edilmektedir.

6102 sayılı Yeni TTK ekonomimizin önemli unsurlarında olan Anonim Şirketler için evrensel ilkeleri temel alan önemli düzenlemeler getirmiş özellikle bu tür şirketlerin sağlam finansal yapılara sahip olmasını sağlamada önemli rolü olan kurumsal yönetim ilkelerini referans almıştır. Bu kapsam Anonim Şirketlerde finansal tabloların Uluslararası Finansal Raporlama Standartlarına uygun şekilde düzenlenmesi sağlam iç kontrol sistemlerinin kurulması ve bağımsız denetimin getirilmesi risk yönetimi gibi konulara ilişkin önemli düzenlemeler kamunun en çok dikkatini çeken düzenlemelerdir.

Belirli pay sahiplerine ve azlığa yönetim kurulunda temsil edilebilme hakkı verilebilmesi, tek kişilik anonim şirket kurulabilmesi, ortaklara şirketten borç alma yasağı getirilmesi, finansal bilgilerin internet ortamında ilan edilebilmesi, yönetim kurulu üyelerinin niteliğine ilişkin düzenlemelerde en az dörtte birinin yüksek öğrenim görmesi, yönetim kurulu üyelerinin elektronik ortamda toplantıya katılabilme imkanı getirilebilmesi gibi diğer düzenlemelerde yenilik niteliği taşıyan düzenlemelerdir. Hiç şüphesiz ki bu düzenlemeler risk yönetimi ve iç denetim açısından kurumun içsel ortamı ve örgütsel yapılanmasını etkileyen önemli değişikliklerdendir.

Konumuz açısından burada en önemli nokta Anonim Şirketlerde yönetim kuruluna getirilen sorumluluklarda 6102 sayılı TTK 375 nolu yönetim kurulunun devredilemez görev ve yetkileri maddesinde yer alan esaslar aşağıdaki gibidir.

6102 sayılı kanunun 366 nolu maddesinde ‘’yönetim kurulu işlerin gidişini izlemek kendisine sunulacak konularda rapor hazırlamak kararları uygulatmaya iç denetim amacıyla içlerinde yönetim kurulu üyelerinin de bulunabileceği komiteler ve komisyonlar kurabilir’’ hükmü yer almaktadır.

Bu konuda yer verdiğimiz bu iki madde diğer maddelerle birlikte değerlendirildiğinde işletme yönetimlerinin iç denetim birimi yada fonksiyonu oluşturmaları bir gereklilik olarak karşımıza çıkmaktadır.

Kanunun konumuz açısında diğer bir önemli maddesi de halka açık şirketler için ‘’Riskin Erken Saptanması ve Yönetimi’’ ile ilgili 378. Maddesidir. Buna göre ;

‘’Pay senetleri borsada işlem gören kurumlarda, 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 kurumlarda bu komite denetçinin gerekli görüp bunu yönetim kuruluna yazılı olarak bildirmesi hâlinde derhâl kurulur ve ilk raporunu kurulmasını izleyen bir ayın sonunda verir. Komite, yönetim kuruluna her iki ayda bir vereceği raporda durumu değerlendirir, varsa tehlikelere işaret eder, çareleri gösterir. Rapor denetçiye de yollanır.’’[130]

Ticari hayatımıza bir çok yenilik getiren, 6102 sayılı Türk Ticaret Kanunu, 13/1/2011 tarihinde kabul edilerek 14/2/2011 tarihli ve 27846 sayılı Resmi Gazete'de yayımlanmıştır. Kanun'un; internet sitesi kurulmasına, ticari defterlerin Türkiye Muhasebe Standartlarına göre tutulmasına, Anonim ve Limited şirketlerin bağımsız denetime tabi olmalarına ilişkin hükümleri dışında kalan düzenlemeleri 1/7/2012 tarihinde yürürlüğe girmiştir.

Yeni Türk Ticaret Kanunu'nun getirdiği yenilikler; ticari hayatın çağa ayak uyduracak şekilde düzenlenmesi ve ticaretin önündeki engellerin kaldırılması, gerçek ve tüzel kişi tacirler ile bunlarla ticari ilişki içerisinde bulunan üçüncü şahısların haklarının

[130] TTK Madde 378

korunması bakımından büyük kolaylıklar sağlayacaktır. Ayrıca yapılan düzenlemeler ticaret hayatını baştan sona değiştireceği gibi vergi ve muhasebe uygulamaları açısından da önemli değişiklikler yapacaktır. İşletmelerin mali tablolarını Türkiye Muhasebe Standartlarına uygun hazırlaması, bağımsız denetim, tutulacak defterler, ortakların ortağı olduğu şirkete borçlanmalarının yasaklanması, ticari karları ile üzerinden vergi hesaplanan kazançlarının ayrı ayrı hesaplanması gerekliliği ve birçok maddeye uyulmaması durumunda adli ya da hapis cezası verilmesi gibi yenilikler muhasebeye verilen önemi artıracaktır.

3.2. TTK ile Getirilen Düzenlemeler Kapsamında İç Denetimin Gerekliliği

Yukarıdaki maddelerde zımni olarak yer verilen iç denetime yönelik maddeler çerçevesinde Anonim Şirketlerde iç denetim gereklilikleri hususunda şu analizi yapmak mümkündür;

Esasen kanunda iç denetim konusunda açık bir atıf bulunmamakla birlikte; iç denetim sisteminin kurulmasını gerektirecek bazı unsurlar yasanın muhtelif maddelerinde ve gerekçesinde yer almaktadır. Bu konuda en net atıf, yasanın yukarıda açıkladığımız "Risklerin Erken Saptanması ve Giderilmesi" ni düzenleyen 378. Maddesinin gerekçesinde yer almaktadır. Yasaya göre "pay senetleri borsa da işlem gören kurumlarda, yönetim kurulu, kurumun 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." Maddenin gerekçesinde söz konusu komite "diğer bir iç denetim mekanizması" olarak öngörülmektedir.

366. madde de yönetim kurulunun "...işlerin gidişatını izlemek, kendisine sunulacak konularda rapor hazırlamak, kararlarını uygulatmak veya iç denetim amacıyla içlerinde yönetim kurulu üyelerinin de bulunabileceği komiteler ve komisyonlar kurulabilir" denilmektedir.

Maddede yer alan "denetim komitesinin diğer görevlerinin yanı sıra bizzat kendisinin iç denetim yapması mümkün olmayacağından bu ifadenin kurum içerisindeki iç denetim sisteminin gözetiminin yapılmasını kastettiği düşünülebilecektir. Yasanın birçok yerinde "iç denetim" ve "diğer bir kontrol mekanizması" gibi ifadelerle ulusla-

rarası alandaki kavramlara atıf yapılmakla birlikte; neyin kastedildiği dahi açık ifade edilmemektedir. Dolayısıyla söz konusu kavramların uluslararası kullanımlarına bakılarak kastedilen hususlar hakkında varsayımlar yoluyla değerlendirme yapmak mümkün olabilir.[131]

TTK'da 367. Madde de yönetimin yetki devri konusu düzenlenirken bu devrin bir iç yönerge ile yapılabileceği öngörülmektedir. 369. Madde de denetim ortamının önemli unsurlarından biri olan etik değerler ve dürüstlük kavramına değinilmekte "yönetim kurulu üyelerinin ve yönetimle görevli üçüncü kişilerin şirketin menfaatlerini görevlerini dürüstlük kurallarına uyarak gözetmek yükümlülüğü altında oldukları" ifade edilmektedir.

375. Madde de yönetim kurulunun devredilemez yetkileri etkin bir iç denetim sisteminin unsurlarını tarif etmekte ancak iç denetim kavramı ile doğrudan ilgisini kurmamaktadır. Bu ilgi, tarafımızca iç denetim kavramının içeriği ile ilgili maddenin içeriği arasındaki benzerlikler aracılığı ile yapılmaya çalışılacaktır. Söz konusu madde de yer alan hususların ağırlıklı olarak kurumsal yönetim prensiplerinde yer alan yönetim kurullarının görevlerini büyük ölçüde yansıtmasının yanı sıra iç denetim sistemi kapsamında yönetim kurulunca yerine getirilmesi gereken hususlara işaret ettiğini söylemek mümkündür. 375. Madde de yer alan hususlar ile yönetim kurullarının iç denetim kapsamındaki sorumluluklarına ilişkin uluslararası terminolojinin karşılaştırılması halinde bazı benzerlikler görülmektedir. "Kurumun üst düzeyde yönetimi ve bunlarla ilgili talimatların verilmesi" hususu iç denetim sisteminde yönetim kurullarının kurum faaliyetlerine yönelik rehberlik etme ve en üst düzeyde çalışma ortamının oluşturulması ile alt başlığı yakından ilgilidir. Nitekim, maddenin gerekçesinde "üst düzey yönetim ile kastedilen, genel işletme politikası başta olmak üzere, yatırım, finansman, temettü gibi politikaların hedeflerinin karara bağlanması, bunlara ulaşılması için seçilen araçların gösterilmesi, hedeflere ulaşılıp ulaşılmadığının veya ulaşılıp ulaşılamayacağının belirlenmesi, bütçe uygulamasının kontrolü ve stratejilerinin tespitidir" açıklaması getirilmektedir.

"Kurum yönetim teşkilatının belirlenmesi" yine yönetim kurulunun üst düzey yöneticilere rehberlik etme sorumluluklarından bir diğerini temsil etmektedir. Maddenin gerekçesinde "örgüt şeması yönetimde yer alan herkesin, altlık-üstlük ilişkilerini, görev

[131] TTK Madde 378

tanımlarını; bölümleri ve aralarındaki ilişkileri gösteren şemadır. Bu hükümle, yönetim kurulunun, yönetimin bir bütün halinde işleyişini görmesi, politikaların ve stratejilerin gerçekleştirilmesinde görevlilerin rolünü değerlendirmesi; insan kaynaklarının kullanılmasını izlemesi amaçlanmıştır. Şema sistemin işleyişindeki aksaklıkların ve aksayan yerin belirlenmesine yardımcı olur" denilmek suretiyle iç denetim modellerinde "bilgi ve iletişim" adımları ile açıklanmaya çalışılan her çalışanın görevlerine ilişkin rol ve sorumluluklarını bilmesi gerektiği koşulu zımnen yerine getirilmektedir.

375. maddenin 1. Fıkrasının (e) bendi yine iç denetime ilişkin uluslararası uygulamalarda görülen bir düzenlemeye işaret etmektedir. İlgili bent, yönetim kurulunun devredilemez görevleri arasında "Yönetimle görevli kişilerin, özellikle kanunlara, esas sözleşmeye, iç yönergelere ve yönetim kurulunun yazılı talimatlarına uygun hareket edip etmediklerinin üst gözetimini de saymaktadır. Bu madde ile birçok kurumsal yönetim prensibinde yer alan yönetim kurullarının kurum faaliyetlerine yönelik gözetim sorumluluğunun kastedildiği söylenebilecektir. Bu üst gözetimin yapılması ise etkin bir iç kontrol sistemi ile iç denetim sistemine ihtiyaç gösterecektir.

375. maddenin (c) bendi iç kontrol ve iç denetim sistemleri ile en yakından ilişkili bendi oluşturmaktadır. "Muhasebe, finans denetimi ve şirketin yönetiminin gerektirdiği ölçüde, finansal planlama için gerekli düzenin kurulması" yönetim kurulunun denetim konusundaki sorumluluklarının alt yapısını oluşturmaktadır. Finansal denetim düzeninin kurulması belki de yasanın kurumlarda iç denetim ve iç kontrol sistemleri ile en yakından ilişkili bölümünü oluşturmaktadır. Finans denetimine ilişkin maddenin gerekçesinde şu açıklamalar yapılmaktadır;

"Finansal denetim düzeninin kurulması, kurumun işlemlerinin denetlenmesine ilişkin bir iç denetim sisteminin ve bunu yapacak örgütün gösterilmesidir. Şirket hangi büyüklükte olursa olsun şirkette, muhasebeden tamamen bağımsız, uzmanlardan oluşan, etkin bir iç denetim örgütüne gereksinim vardır. Bir anonim şirketin denetimi sadece bir bağımsız dış denetim kuruluşuna bırakılamaz. Bir bağımsız denetim kuruluşunun onlarca hatta yüzlerce müşterisi vardır; onlara birçok hizmet sunmaktadır. Her müşterisini içeriden ve yakından izleyemez. Finansal denetim bir anlamda "Teftiş Kurulu" nun yaptığı denetimdir. Finansal denetim iş ve işlemlerin iç denetimi yanında, şirketin finansal kaynaklarının, bunların kullanılma şeklinin durumunun, likiditesinin

denetimini ve izlenmesini de içerir. Finansal denetim kurumsal yönetim kurallarının gereğidir."

İlgili yasa maddesinin gerekçesinde iç denetim sistemine doğrudan bir atıf yapılmaktadır. Finansal süreçlerle ilgili yasada olmasa bile gerekçesinin bir iç denetim sistemini ve buna bağlı olarak finansal süreçlere yönelik bir iç kontrol sisteminin varlığını en kesin ifadelerle öngördüğü kısmı burası olmaktadır. Dolayısıyla, yukarıdaki gerekçenin kurumlarda etkin bir iç denetim sistemi kurulması ve idame ettirilmesinin temel gerekçesini oluşturduğu söylenebilecektir.

Maddenin (f) bendinde, "...yıllık faaliyet raporunun ve kurumsal yönetim açıklamasının düzenlenmesi..." yönetim kurulunun devredilemez görevleri arasında yer almaktadır. 516. madde de ise, yönetim kurulunun yıllık faaliyet raporunun, yasada belirtilen diğer hususların yanı sıra "şirketin gelişmesine ve karşılaşması muhtemel risklere de açıkça işaret olunması" gerekli kılınmaktadır.

Dünyaya hızla açılan ve her geçen yıl büyüyen ekonomisiyle ve kurumlarıyla global bir oyuncu haline gelen ülkemizdeki kurumların tüm dünyada geçerli olan yönetim ilke ve prensipleriyle yönetilmesi, ulusal ve uluslararası rekabet gücünü koruyabilmek için bir gereklilik olmaktadır. Global alanda yönetim kurulları için geçerli olan rol ve sorumluluklar ülkemiz kurumları içinde geçerlidir.[132]

Ülkemiz kurumları da diğer ülke kurumlarında olduğu gibi belirli mevzuata uymak zorunda olmanın yanı sıra operasyonel, finansal hedeflere sahip olup yine diğer ülke kurumlarıyla benzer risklerle karşılaşabilmektedirler. Söz konusu risklerin yönetilmesi yine diğer ülke kurumlarında olduğu gibi etkili bir yönetim kurulu rehberliğini ve gözetiminin yanı sıra etkin bir iç kontrol ve iç denetim sisteminin varlığını gerekli kılmaktadır. Bütün gelişmiş ve gelişmekte olan ülkelerin ilgili yasal düzenlemelerinde söz konusu sistemlere yer verildiği görülmektedir.

Bu değerlendirmeler bize Yeni TTK 'nın örtülüde olsa yöneticilerin sağlam iç kontrollerden kaynaklanan sorumluluklarını gereği gibi yerine getirmelerinde kendilerine yardımcı olacak erken uyarı sistemlerini dolayısıyla iç denetim birimi oluşturmalarının gereğini ortaya koymaktadır.

---

[132] Arzu Pişkinoğlu; **"Operasyonel Risk Yönetiminde Yaşanan Gelişmeler''**, Active, Kasım -Aralık 2003.s.24.

BÖLÜM IV

ANONİM ŞİRKETLERDE İÇ DENETİM BİRİMİNİN YAPILANDIRILMASI VE RİSK YÖNETİMİNDEKİ ROLÜ ÜZERİNE BİR UYGULAMA ÖRNEĞİ

4.1. Uygulamanın Amacı

Tezin bu bölümünde KRY süreci ve bu süreçte iç denetçinin rolü bir uygulama örneği üzerinde incelenmiştir. Bu amaçla KRY yapılandırma sürecinde olan KLM A.Ş. seçilerek sürecin aşamaları rol ve sorumlulukları gösterecek şekilde açıklanmış bu şekilde somut bir örnek verilmeye çalışılmıştır.

4.2. Kurum İle İlgili Genel Bilgiler

2012 yılında, ilköğretim ünite dergileriyle yayın hayatına başlayan KLM A.Ş. ürün yelpazesini kısa süre içinde genişletmiş, sektöründe öncü bir kurum olarak yerini almıştır. Okul öncesi, ilköğretim, ortaöğretim yayıncılığı ve sınav hizmetleri olmak üzere dört farklı alanda faaliyet gösteren şirket, 2012 yılı itibari ile, 550' nin üzerinde ana bayi ve ana dağıtım kurumları aracılığıyla 2000' in üzerinde satış noktası ile Türkiye'nin dört bir yanına ulaşmaktadır. Ayrıca Türkiye'nin 150'ye yakın Ülkede yayıncılık yapan tek markasıdır.

31 Aralık 2012 itibariyle KLM A.Ş. ‘nin toplam cirosu 137,9 Milyon TL ve net karı 21,6 Milyon TL, personel sayısı ise 136 ‘dır.

4.3. KRY İle İlgili Hazırlık Çalışmaları

Öncelikle süreçte İç Denetim Birimi danışmanlık rolü kapsamında dışarıdan tasarım hizmeti veren bağımsız denetim ekibi ile birlikte görev almıştır. Bu kapsamda oluşturulan denetim ekibi KLM A.Ş. ‘nin Genel Müdür Yardımcısı, Üst düzey yöneticileri ve orta düzey yöneticileri ile bir randevu alarak şirket personelinin risk envanterini çıkarmayı planlamıştır. Bunun için öncelikle Genel Müdür Yardımcısı ve diğer personel ayrı ayrı değerlendirmeye tabi tutulmuştur. Çünkü denetim ekibi tarafından elde edinilecek risklerin doğruluğu ve güvenilirliği açısından alt personelin Genel müdür yardımcısından etkilenmesi istenmemiştir.

Genel Müdür Yardımcısı ve diğer personel yetkilileriyle görüşmeler sonucunda uygun tarihlerde randevu alınmış olup tüm katılımcılara risk yönetiminin gerekliliği ve temel unsurları genel olarak anlatılmaya çalışılmıştır.

Uygulama evreleri en güncel ve uluslararası alanda en çok kabul gören KRY Kübü bileşenleri kapsamında değerlendirmeye tabi tutulmuştur. Bu evreler sırasıyla aşağıda açıklanmıştır.

4.3.1. Kontrol Ortamı

Etkili bir KRY sisteminin kurulması, önce söz konusu sistemin kurulacağı çalışma ortamının mevcut durumunun değerlendirilmesini ve gerekli olması halinde kuvvetlendirilmesini gerektirecektir.

KRY' in başarılı olmasının ön koşullarından birisi kurumun her seviyesinde bir risk farkındalığının olup olmadığıdır. Bu kapsamda kurum çalışanlarına aşağıdaki sorular sorulmuştur.

- Kurum çalışanları risk kavramının ne olduğunu bilmekte midir?
- Kurum hangi faaliyetlerinde hangi tür risklerle karşı karşıyadır veya gelecekte kalabilecektir?
- Söz konusu riskin gerçekleşmesi olasılığı nedir?
- Gerçekleşmesi halinde yaratacağı olumsuz sonuçlar neler olabilir?
- Bu zararı önlemek için hangi tür kontrol önlemleri alınabilir veya varsa mevcut önlemler ne kadar etkindir?
- Her kademe yönetici ve çalışanlar anlık veya günlük olarak aldıkları tüm kararlarda yukarıda bahsedilen unsurları göz önünde bulundurmakta mıdırlar?

Tüm bu soruların cevaplandırılması mevcut ortamın ve çalışanların risk farkındalıklarının bir değerlendirmesinin yapılmasını gerektirecektir.

Bu amaçla denetim ekibi tarafından Risk Yönetimi konusunda ortak bir dil ve felsefe geliştirmeye çalışılmıştır. KLM A.Ş.'nin yazılı misyon ve vizyon metinleri oluşturması ve bunu tüm teşkilat ve kurum dışıyla paylaşması , ayrıca tek sayfalık bir risk yönetimi felsefesi olarak da yapılabilecektir. Bu metin, aynı zamanda, kurumun risk iştahının tüm teşkilatla paylaşılması için etkin bir yöntemdir. Metinde risk kavramının

önemi ve verebileceği zararlar, etkin bir risk yönetim sisteminin kuruma sağlayacağı fayda, yönetim kurulu ve üst yönetimin bu konudaki uzun dönemli kararlılığı ve tüm sistemin başarıyla kurulması ve tüm çalışanların beklentilerine yer verilmiştir. Her çalışan, KRY sisteminin kurumun kârlılık, üretim, satış ve diğer hedeflerini gerçekleştirmesi, operasyonlarının verimliliğini artırması ve bir bütün olarak kuruma ne tür katkılar sağlayacağı konusunda yeterli bilgiye sahip olmanın yanı sıra sistemin işlerliği için kendisine düşen rol ve sorumlulukları hakkında bilgilendirilmiştir.

4.3.2. Amaçların Belirlenmesi

Ön çalışma aşamasında denetçi uygun denetim bulgularını elde edeceğinden emin olmak için öncelikle denetimin amaçlarını belirleyecektir.

Ana stratejik hedefler, söz konusu vizyon ve misyonun gerçekleştirilmesini sağlayacak kurumun en üst düzeydeki hedefleridir. Kurumun vizyonunun daha somutlaştırılmış hali olup vizyonda belirtilen noktaya ulaşmak için birer yol haritası niteliğindedir. Dolayısıyla kurum vizyonu ile aralarında çok yakın bir ilişkinin ve bütünlüğün olması gerekmektedir.

Denetim ekibi, KLM Anonim Şirketi için söz konusu stratejik hedefler ve kritik başarı faktörleri belirlenirken bir önceki yıl şirket üst yönetimi tarafından belirlenen önemli kriterler göz önünde bulundurularak aşağıdaki şekilde belirlenmiştir.

Şekil 8 – Ana Stratejik Hedefler

4.3.3. Olayların Tanımlanması

KRY' e göre iki ana belirsizlik kaynağı dışsal ve içsel faktörlerdir. Dışsal faktörler kurumun faaliyette bulunduğu ekonomik, sosyal, yasal ortamdan kaynaklanan faktörleri ifade etmekte, içsel faktörler ise kurumun finansal yapısı, organizasyonel yapılanması insan kaynağı ve kullandığı teknolojiler gibi kendisinden kaynaklanan olayları ifade etmektedir.

Söz konusu içsel ve dışsal faktörlerin neden olabileceği olaylara risk veya kurumlar ise aşağıdaki hususlar örnek olarak verilmektedir.

Dışsal Faktörler; Enflasyon, işsizlik ve işgücü piyasası, dış ticaret, ekonomik büyüme, ekonomik istikrar, hammadde, enerji fiyat ve tedarik koşullarındaki gelişmeler, global ekonomik büyümedeki artış veya azalışlar, global ticaretteki gelişmeler, komşu ülkelerdeki ekonomik gelişmeler, olası bir global kriz, global likidite koşulları, global yatırım ortamındaki değişimlerdir.

İçsel Faktörler; Kurum altyapısından kaynaklanan faktörler, hataların azaltılmasını engellemek amacıyla altyapı yatırımlarına yatırım yapılma ihtiyacı, çağrı merkezi yatırımı, yenileme yatırımları, nitelikli insan kaynağı ve anahtar yöneticilerin değişimleri, operasyonların karmaşıklık seviyesi; teknoloji yoğun veya işgücü yoğun üretim tekniklerinin ağırlığı sıralanabilinir.

Denetim ekibi tarafından KLM Anonim Şirketi'nin Genel Müdür ve Genel Müdür Yardımcısı ile yapılan görüşmeler sonucunda belirlemiş olduğu finansal, operasyonel ve stratejik hedefler aşağıdaki tabloda iç ve dış kaynaklı olacak şekilde gruplanarak özetlenmiştir.

Bu hedeflere bakıldığında, bütçe ve karlılık hedeflerinin yakalanması, müşteri memnuniyetinin üst seviyede tutulması gibi hedefler KLM A.Ş.' nin iç kaynaklı finansal ve operasyonel hedeflerini oluşturmaktadır.

Tablo 1-Hedeflerin Belirlenmesi

HEDEF / RİSK GRUBU	KAYNAK	AMAÇLAR	KRİTİK BAŞARI FAKTÖRLERİ
FİNANSAL	İÇ KAYNAKLI	Bütçe ve Karlılık Hedeflerinin Yakalanması	(- %5 sapma ve altında bütçeyi yakalamak) Karlılık Hedefi Giderler Hedefi Ciro Hedefi
FİNANSAL	İÇ KAYNAKLI	Bütçe ve Karlılık Hedeflerinin Yakalanması	(- %5 sapma ve altında bütçeyi yakalamak) Karlılık Hedefi Giderler Hedefi Ciro Hedefi
FİNANSAL	İÇ KAYNAKLI	Bütçe ve Karlılık Hedeflerinin Yakalanması	(- %5 sapma ve altında bütçeyi yakalamak) Karlılık Hedefi Giderler Hedefi Ciro Hedefi
OPERASYONEL	İÇ KAYNAKLI	Müşteri memnuniyetini üst seviyede sağlamak	Ürünlerin zamanında gitmesi Ürünlerin zamanında üretilmesi Hatasız ürün, Tercih edilen olmak

Tablo 2- Hedeflerin Belirlenmesi (Devam)

HEDEF / RİSK GRUBU	KAYNAK	AMAÇLAR	KRİTİK BAŞARI FAKTÖRLERİ
STRATEJİK	DIŞ KAYNAKLI	Değişimi (sektör içindeki ve sektörler arası) sağlıklı yönetmek, hızlı ayak uydurmak	Değişime hızlı bir şekilde tepki verip, yeni ürünleri koymak, değişimi yönetememek
UYUMLULUK	DIŞ KAYNAKLI	Değişen mevzuata uyum	Ürünlerin hızlı bir şekilde değişime hazır hale getirilmesi Ürünleri hızlı toplamak
STRATEJİK	İÇ KAYNAKLI	Dijital ortamdan yayınlara ulaşabilirlirliğin arttırılması	Mevcut yayınların %100 dijital ortama taşınması Tolerans: -%10
OPERASYONEL	İÇ KAYNAKLI	Karlılık, maliyet ve nakit akışı hedeflerine uygun esereler ile ulaşılması	Kitapların %100 uygun eserlerden oluşması Bütçe ve karlılık hedeflerine %100 ulaşması
OPERASYONEL	DIŞ KAYNAKLI	Karlılık, maliyet ve nakit akışı hedeflerine uygun esereler ile ulaşılması	Kitapların %100 uygun eserlerden oluşması Bütçe ve karlılık hedeflerine %100 ulaşması
FİNANSAL	İÇ KAYNAKLI	Tiraj ve ciro hedeflerinin tutturulması	Tiraj ve ciro hedeflerinin %100 yakalanması Tolerans: %10
STRATEJİK	DIŞ KAYNAKLI	Dergilerin okunulurluğunun arttırılması	- Çağrı merkezi örneklem sonuçlarının analizi - Dergi içeriğinde gerekli oranların yakalanması - Okur yarışmaları katılım oranı
UYUMLULUK	İÇ KAYNAKLI	Dergi tahsilatlarında yasal uyumun sağlanması	- Dergi tahsilatlarında abonelerden yapılan tahsilatın %60'a çıkarılması Tolerans: - %10

Tablo 3- Hedeflerin Belirlenmesi (Devam)

HEDEF / RİSK GRUBU	KAYNAK	AMAÇLAR	KRİTİK BAŞARI FAKTÖRLERİ
FİNANSAL	DIŞ KAYNAKLI	Bütçe ve karlılık hedeflerinin yakalanması	Bütçe ve karlılık hedeflerinin %100 yakalanması Tolerans: -%5
FİNANSAL	İÇ KAYNAKLI	Sürdürülebilirlik	Tahsilat hızının ortalama 30 günde tahsil edilebilmesi Tolerans: +20 Gün
OPERASYONEL	İÇ KAYNAKLI	İşlemlerin ve süreçlerin tamamının standartlar çerçevesinde gerçekleştirilmesi	Şirketin ana süreçlerinin %70 oranında politika ve prosedürler ile tanımlı hale getirilmesi Tolerans: %10
OPERASYONEL	İÇ KAYNAKLI	Kaliteli ve uygun niteliklere sahip insan kaynağının istihdam edilmesi	Personel devir hızının %5 olması Tolerans: + / - %10
OPERASYONEL	İÇ KAYNAKLI	Kaliteli ve uygun niteliklere sahip insan kaynağının istihdam edilmesi	Personel devir hızının %20 olması Tolerans: + / - %5
UYUMLULUK	İÇ KAYNAKLI	Yasal mevzuata tam uyum	Yasal mevzuata %100 uyum Yasal veya vergisel 0 ceza Tolerans: -%5
UYUMLULUK	İÇ KAYNAKLI	Şirketin hak ve yükümlülüklerini tam olarak koruması ve yerine getirmesi	Yapılan sözleşmelerin tamamının Hukuk Koordinatörlüğü onayından geçmesi Tolerans: %5

Tablo 4- Hedeflerin Belirlenmesi (Devam)

HEDEF / RİSK GRUBU	KAYNAK	AMAÇLAR	KRİTİK BAŞARI FAKTÖRLERİ
FİNANSAL	DIŞ KAYNAKLI	Bütçe ve karlılık hedeflerinin yakalanması	Bütçe ve karlılık hedeflerinin %100 yakalanması Tolerans: -%5
STRATEJİK	İÇ KAYNAKLI	Yurt dışı satışlara odaklanılması	yurt dışı satışların payının %30 arttırılması Tolerans: % 5
FİNANSAL	DIŞ KAYNAKLI	Bütçe ve karlılık hedeflerinin yakalanması	Bütçe ve karlılık hedeflerinin %100 yakalanması Tolerans: -%5
OPERASYONEL	İÇ KAYNAKLI	Operasyonların etkin ve efektif bir şekilde gerçekleştirilmesi	Stok kayıplarının toplam giderin %5'inin altında olması Tolerans: %5
OPERASYONEL	İÇ KAYNAKLI	Operasyonel kaliteyi arttırmak	Personel devir hızının %5 olması Tolerans: + / - %5
OPERASYONEL	İÇ KAYNAKLI	Operasyonel kaliteyi arttırmak	Geç hasarlı teslimat oranının ve maliyetinin %5 in altında gerçekleşmesi Tolerans: %5
OPERASYONEL	İÇ KAYNAKLI	Lojistik alanında sürdürülebilir yapıyı kurmak ve büyütmek	Bütçenin ve operasyonel performans hedeflerinin %100 yakalanması (palet, ciro, karlılık) Tolerans: - %5

Risk toleransı kurumun tüm faaliyetlerine ve işlem süreçlerine yönelik olarak birbiriyle uyumlu ve kurumun genel risk iştahını yansıtacak şekilde çok sayıda belirlenebilir.

Buna karşın, değişen mevzuata uyum, dergilerin okunabilirliğinin arttırılması, değişen sektörlere uyum, müşterilerden tahsilat ile ilgili politikaların yasal çerçevelere olan değişimi ve bütçe performanslar finansal ve uyumluluk hedeflerini oluşturmaktadır.

Tüm bu hedefler ışığında bütçe ve karlılık hedeflerine ait kritik başarı faktörlerinin giderler ve ciro gibi hedeflere % 5 tolerans düzeyinde ulaşmak olduğu anlaşılmaktadır.

Müşteri memnuniyetini üst düzeyde sağlama hedefine ait kritik başarı faktörlerini ise ürünlerin zamanında teslim edilmesi ve zamanında üretilmesi, ürünlerinin en az hata ile üretilmesi ve tercih edilen bir sistem kurmak olduğu görülmektedir.

Sürdürülebilir nitelikli insan kaynağına ilişkin hedeflere ait kritik başarı faktörleri ise %10 tolerans düzeyinde devir hızı ve sürdürülebilir tahsilat politikasına ait kritik başarı faktörleri ise 30 gün tolerans düzeyinde gerçekleşmiştir.

KLM A.Ş. ye ait tüm hedeflere bakıldığında diğer hedeflerden farklı olarak kitap tiraj sayılarına ve yasal mevzuata uygun eserler çıkarma toleransları sıfır olarak belirlendiği göze çarpmaktadır.

4.3.4. Risklerin Değerlendirilmesi

Özellikle kurumun ana stratejik hedefleri veya her birimin kendi hedefleri ortaya konduktan sonra yapılması gereken, genel bir risk envanteri çıkarmak değil, hangi hedefi hangi riskin etkileyebileceğini tahmin etmeye çalışmak olacaktır.

Diğer bir deyişle, ayrı ayrı hedef ve risk envanterleri çıkarılarak değil hedeflerle bu risklerin ilişkisinin de ortaya konularak hangi riskin hangi hedefi etkileyebileceğinin de bu çalışmalar sırasında tahmin edilmeye çalışılması gerekmektedir.

Bu amaçla denetim ekibi tarafından yapılan mülakatlarda İkinci Bölümde açıklanan içsel ve artık riskler Tablo-5 ve Tablo-6 ‘ aktarılmıştır.

4.3.4.1.İçsel ve Artık Riskler

Tablo 5- Risklerin Sınıflandırılması

İÇSEL RİSKLER	ARTIK RİSKLER	Etkilenen
Bütçenin Etkin ve Verimli Yönetilememesi	- Hedefler belirlenirken detaylı / gerçekçi belirlenememesi - Bütçe programının etkin ve verimli yönetilememesi - Maliyetin altında satışlar - MEB politikaları	Tüm Şirket Birimleri
Başarının kanıksanması	- Bazı ürün satışlarına daha fazla önem verilirken Bazı Ürünlerin geri planda kalması '- Hedefe etkisi belirlenmeden yatırımlar yapılması (TEDES)	Tüm Şirket
İnsan Kaynakları yönetiminin etkin ve verimli yapılamaması	- Çalışanların motivasyon durumu - Terfi ve ücretlendirme sisteminin motivasyona negatif etkisi olması (eşitlik)	Tüm Şirket
	- Performans sisteminin oluşturulamaması - Yönetim ani değişikliği sonucu ani sistem değişiklikleri	Tüm Şirket
Müşteri memnuniyetini üst seviyede sağlanamaması,	- Ürünlerin zamanında üretilememesi veya hatalı üretim yapılması, Doğru kriterlerdeki kitapların basılıp yayınlanmaması - Ürünlerin Zamanında gitmemesi	Müşteri
Etkin bir Tahsilat Politikaların Yönetilememesi	- Tahsilatların zamanında gerçekleştirilememesi - Müşterilerden teminat alınamaması - Müşteri çek/senet vade ertelemeleri (Temdit) - Kendi gücümüzün farkında olmamak	Şirket

Tablo 6- Risklerin Sınıflandırılması (Devam)

İÇSEL RİSKLER	ARTIK RİSKLER	Etkilenen
Politikaların yazılı hale getirilmemesi	- Politikaların yazılı hale getirilmemesi (Vade ve Iskonto politikasına) '- Yetki ve sorumlulukların net belli olmaması,	Tüm Şirket Birim
Ürün ve Stok yönetiminin etkin ve verimli yapılamaması	- Stokların ekonomik düzeyde gerçekleşmemesi - Depolama ve sevkiyat konusundaki zaafiyet - Baskı adetlerinin optimum belirlenememesi (ilk ve Ek Baskı)	Tüm Şirket
	- Maliyet sisteminin altyapısının kurulmaması	Tüm Şirket
Stratejik ve kurumsal yönetimin etkin yapılamaması	- Stratejik planlamanın olmaması - Merkez karar verme sürecinin doğru ve hızlı işleyişinin sağlanamaması (İnsiyatif alma/almama, karara alma/almama)	Tüm Şirket
	- Acil durum senaryolarının bulunmaması	Tüm Şirket
	- Marka yönetiminin profesyonelce yapılamaması - Marka değerinin farkında olunmaması	Tüm Şirket
Mevzuat değişikliklerinin/uyumunun etkin yönetilememesi	Elektronik yayıncılık (pozitif Yönde etkisi var)	Tüm Şirket
	Eğitim politikalarındaki değişiklik / belirsizlik ve Müfredat değişikliği (MEB	Tüm Şirket
Maliye politikalarındaki değişiklikler	Yeni kanuni düzenlemelere uyumun yasaların tanımış olduğu sürelerde sağlanamaması - TTK, Borçlar kanunu ve benzeri düzenlemeler yapılamaması	Tüm Şirket

Risklerin yönetilmesi için alman kontrol önlemleri söz konusu risklerin gerçekleşme olasılığını azaltabileceği gibi yaratacağı olumsuz etkilerinde azaltılmasını sağlayabilirler. Bir risk için hem gerçekleşme olasılığını azaltın hem de yaratacağı etkiyi azaltıcı ayrı ayrı kontrol önlemleri alınabilir. Sonuçta alınan bu tek veya birden fazla önlemin amacı söz konusu riskin gerçekleşmesi halinde yaratacağı hasarın en aza indirilmesidir.

5.3.4.2. Olasılık-Etki Analizi

Risk yönetiminde üzerinde mutabık kalınan bir değerleme yöntemi risklerin gerçekleşme olasılıkları ve yaratacakları etkiler dikkate alınarak değerlendirilmesidir.

Risklerin gerçekleşme olasılığı hangi sıklıkla gerçekleşeceğinin veya hangi yüzde ile gerçekleşeceğinin tahmin edilmeye çalışılmasıdır. Gerçekleşme olasılığı her risk için aynı olmadığı gibi sıklıkla kastedilen zaman süresi de her risk için eşit değildir.

Değerlendirmenin ikinci boyutu ise, söz konusu riskin gerçekleşmesi halinde yaratacağı zararın boyutunun tahmin edilmesidir. Aynı şekilde, her riskin yaratacağı etki de birbirine eşit değildir. Bazı risklerin yaratacağı olumsuz etki göz ardı edilebileceği gibi bazı riskler kurumun varlığını dahi tehlikeye atacak şiddette hasara neden olabilirler.

Derecelendirme sisteminde en düşükten en yükseğe kademeli olarak artan bir derecelendirme yapılmaktadır. Gerçekleşme olasılığı veya etkisi en düşük olan risklere 1 den başlayarak derece veya puan verilmekte, göreceli olarak gerçekleşme olasılığı veya etkisi daha yüksek olan risklere 2 puan verilmekte ve bu şekilde olasılığı en yüksek risklere doğru en yüksek puan olarak 5 puana kadar bir derecelendirme yapılmaktadır.

KLM Şirketinde düzenlenen seminerde katılımcılara gerçekleşme olasılığını ve etki derecelerinin anlamaları açıklanmaya çalışılmış olup ayrıca her katılımcıya aşağıdaki kartlar dağıtılmıştır. Katılımcılar risk puanlarını denetçiye belirtirlerken bu kartlardaki risk anlamları kendilerine ne ifade ediyorsa ona göre değerlendirmede bulunacaklardır.

Tablo 7- Etki Skalası

Etki Derecesi	Tanım	Açıklama	Örnek Sonucu
5	Katastrofik	İlgili hedef göz önüne alındığında, risk hedefin gerçekleşmesini önleyip, şirketin diğer hedeflerine ve şirket sürekliliğine tehdit oluşturmaktadır.	İşe alım süreci uzun ve bürokratik olması, işlerde gecikmeye, kalitede düşüşe, müşteri memnuniyetsizliği ve itibar kaybına neden olmaktadır.
4	Kritik	İlgili hedef göz önüne alındığında, risk hedefin gerçekleşmesinie tehdit oluşturmaktadır.	İşe alım süreci uzun ve bürokratik olması, kritik pozisyonların boşalması halinde işlerde gecikmeye, kalitede düşüşe neden olmaktadır ve müşteri memnuniyetsizliği ve itibar kaybına yol açabilmektedir.
3	Orta	İlgili hedef göz önüne alındığında, risk hedefin bazı açılardan gerçekleştirilememesine veya hedefin geç yakalanmasına sebep olabilir.	İşe alım süreci uzun ve bürokratik olması, kritik pozisyonların boşalması, mavi yakadaki bazı pozisyonların geçici olarak işlerini geç tamamlamasına/ fazla mesaisine yol açabilmektedir.
2	Katlanılabilir	İlgili hedef göz önüne alındığında, risk hedefin gerçekleştirilememesinde önemli bir etkiye sahip olmayacağı öngörülmektedir.	İşe alım süreci uzun ve bürokratik olması, uygun kişilerin zamanında işe alınmasını geciktirmekle birlikte, önemli bir etkiye sahip değildir.
1	Yoksanabilir	İlgili hedef göz önüne alındığında, risk hedefin gerçekleştirilememesinde farkedilir bir etkiye sahip olmayacağı öngörülmektedir.	İşe alım süreci uzun ve bürokratik olmasının, uygun kişilerin zamanında işe alınmasında bir etkisi olmadığı düşünülmektedir.

Risklerin gerçekleşme olasılığını gösteren bir derecelendirmede puanlar ve anlamları şu şekilde özetlenebilir;[133]

Tablo 8-Olasılık Skalası

5	**Kesin**	İlgili hedef göz önüne alındığında, ilgili zaman periyodunda gerçekleşmesi kesin olarak görülen riskler.	Uzun ve bürokratik işe alım süreci, ihtiyaca uygun yetenekteki çalışanların cezbedilmesini/ işe alınmasını önlemektedir.
4	**Kuvvetle Muhtemel**	İlgili hedef göz önüne alındığında, ilgili zaman periyodunda gerçekleşmesi yüksek ihtimal olarak görülen riskler.	Uzun ve bürokratik işe alım süreci, ihtiyaca uygun yetenekteki çalışanların cezbedilmesini/ işe alınmasında gecikmelere ve fırsatların kaçırılmasına sıklıkla neden olmaktadır.
3	**Muhtemel**	İlgili hedef göz önüne alındığında, ilgili zaman periyodunda gerçekleşmesi beklenen olarak görülen riskler.	Uzun ve bürokratik işe alım süreci, ihtiyaca uygun yetenekteki çalışanların cezbedilmesini/ işe alınmasında gecikmelere ve fırsatların kaçırılmasına neden olmaktadır.
2	**Olası**	İlgili hedef göz önüne alındığında, ilgili zaman periyodunda gerçekleşme ihtimali düşük olarak görülen riskler.	İşe alım süreci uzun ve bürokratik olmasına karşın, ihtiyaca uygun yeteneklerde personel bulunup işe alınmaktla birlikte, kaçırılan fırsatlar da yok değildir.
1	**Olasılık dışı**	İlgili hedef göz önüne alındığında, ilgili zaman periyodunda gerçekleşme ihtimali olmayadığı görülen riskler	İşe alım süreci uzun ve bürokratik olmasına karşın, ihtiyaca uygun yeteneklerde personel bulunup işe alınmaktadır.

[133] Patchin Curtis'' **Coso, Rsk Assessment Practice''** October 2012 s. 5.

4.3.4.3. Risklerin Biraraya Getirilmesi

Risklerin gerek sayısal gerekse sayısal olmayan yöntemlerle etki ve gerçekleşme olasılıklarının değerlendirilmesinden sonra yapılması gereken, bütün risklerin bir araya getirilmesidir. Bir araya getirilen riskler en yüksek gerçekleşme olasılığı ve en yüksek etki açısından bir sıralamaya tabi tutularak hangi risklerin en yüksek gerçekleşme olasılığı ve etkiye sahip olduğu, dolayısıyla öncelikle giderilmesi gereken risklerin neler olduğuna dair bir öncelikli riskler listesine sahip olunacaktır.

Tablo 11, kurumun vizyonuna bağlı olarak, ana stratejik hedefleri ve bu stratejik hedeflere ulaşmak için oluşturulan alt stratejik hedefleri ve bu hedeflere ulaşmak için karşılaşılabilecek olası tüm risklerin bir listesini, hangi riskin hangi hedefi etkileme olasılığı olduğunu, hangi riskin gerçekleşme yüzdesinin daha fazla olduğunu, hangi riskin daha yüksek maddi zarara yol açma riskinin daha yüksek olduğunu bir bütün halinde görmesini sağlayacaktır.

Kurumların bu aşamada aşağıdaki tablolara benzer tablolar oluşturma aşamasında teknolojik imkanlardan faydalanmaları dokümantasyon açısından büyük önem taşıyacaktır. Risk yönetiminde alt kademelere ve alt süreçlere inildikçe dokümantasyon yükü artacaktır. Tek bir tablo oluşturmak yerine birimler veya ana stratejik hedefler bazında tablolar oluşturulması da gündeme gelebilecektir.

KLM A.Ş. ‘de yapılan çalışma neticesinde 3 Genel Müdür Yardımcısı ve 12 üst düzey yöneticinin katıldığı toplantılar sonucunda ana risk ve bunların sonucunda gerçekleşen alt risklere ait olasılık ve etki dereceleri 1 ile 5 puanlar arasında değerlendirmeye tabi tutulmuştur.

Risk puanlamalarının objektif olması açısından Genel Müdür Yardımcıları ve diğer 12 yönetici 2 ayrı grupta toplanarak oylanma yapılması istenmiştir.

Her bir personelin, belirlenen toplam 32 risk faktörüne verdiği puanlamalar Tablo 9 ve Tablo 10 ‘da kaydedilmiştir.

Bu çalışmanın kurumun tüm alt stratejik hedeflerine yönelik yüzlerce alt riski için tüm birimlerce yapılması halinde söz konusu tablonun yüzlerce satırdan oluşan bir tabloya dönüşeceği unutulmamalıdır.

Tablo 9- Risk Puanlaması

KLM ANONİM ŞİRKETİ

KATILIMCILAR

ANA RİSK / ÜST RİSK	RİSK NO	SEBEPLER / KÖK RİSKLER	F. A.		C. A.		İ. İ.		M. K.		A. Ç.		K.A.		M. D.		M. Ö.		S. Ö.		S. Ö.		İ. I.		O.S.		H.G.		F.Ö.		İ.C.		Ortalama Olasılık	Ortalama Etki	Risk Puanı
			O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E			
Bütçenin Etkin ve Verimli Yönetilememesi	1	Hedefler belirlenirken detaylı / gerçekçi belirlenememesi	2	3	2	3	2	3	1	1	2	3	3	2	2	1	2	2	2	3	2	3	2	2	2	1	3	3	2	2	2	3	2	2	4
	2	MEB politikalarındaki değişiklik	4	4	3	3	5	5	3	3	4	4	4	3	3	4	3	4	4	4	3	3	4	4	4	4	4	4	4	4	4	4	4	4	16
	3	Merkezin Bağlayıcı Kararları Bütçe karının % oran bazında verilmesi Sınav-1. setler-O.Ö eğitim setleri	3	3	2	2	3	3	3	3	2	4	3	3	3	3	3	2	3	3	3	3	3	3	4	4	3	3	3	3	2	2	3	3	9
	4	Yatırımlardaki süreçlerinde sapmalar yaşanması	2	3	3	3	2	3	3	3	3	3	2	3	2	3	3	2	2	3	2	3	3	2	3	3	2	3	2	2	2	3	2	3	6
İnsan Kaynakları yönetiminin etkin ve verimli yapılamaması	5	Çalışanların motivasyon durumu	3	3	2	1	1	1	4	4	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	3	2	2	4	4	2	2	3	3	9
	6	Terfi ve ücretlendirme sisteminin motivasyona negatif etkisi olması (eşitlik)	3	4	2	2	2	2	2	2	3	4	3	4	3	3	4	4	3	4	3	4	4	4	3	3	2	3	4	4	3	3	3	3	9
	7	Performans sisteminin oluşturulamaması	3	4	2	2	3	3	3	3	3	4	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	9
	8	Yönetim ani değişikliği sonucu ani sistem değişiklikleri	1	2	2	2	1	1	2	2	3	3	2	2	2	2	1	2	2	2	3	3	2	2	2	2	2	2	2	2	2	2	2	2	4
	9	Kariyer Planlamasının olmaması Çalışanların geçmiş Sicil Kaydının/ Çalışma faliyetrinin etkin yönetilememesi	2	3	3	2	2	2	2	2	2	4	3	4	3	3	3	3	3	3	3	3	3	2	3	3	2	2	3	3	2	2	3	3	9
Müşteri memnuniyetinin üst seviyede sağlanamaması	10	Ürünlerin zamanında üretilememesi veya hatalı üretim yapılması,	3	5	2	3	3	4	4	4	4	5	3	3	4	4	3	4	4	3	3	3	3	4	4	4	3	4	4	4	3	4	3	4	12
	11	Ürünlerin Zamanında gitmemesi	3	4	3	3	3	4	4	4	4	5	3	4	3	4	2	4	4	3	3	4	4	3	2	5	3	4	3	4	2	4	3	4	12
	12	Doğru kriterlerdeki kitapların basılıp yayınlanmaması YGS LYS kitap çıkmaması, Ana sınıf Setlerinin güncellenmesi,	3	5	2	3	4	4	2	2	3	4	4	3	4	3	3	4	3	4	3	4	3	4	2	3	3	4	3	4	3	3	3	4	12
	13	Müşteri Sağlıklı iletişim (BMT), Call Center	2	3	2	2	1	1	4	4	3	2	2	4	2	2	2	4	2	3	3	3	2	3	2	3	2	3	2	3	2	4	2	3	6

KLM ANONİM ŞİRKETİ			KATILIMCILAR																																
			F. A.		C. A.		İ. İ.		M. K.		A. Ç.		K.A.		M. D.		M. Ö.		S. Ö.		S. Ö.		İ. I.		O.S.		H.G.		F.Ö.		İ.C.				
ANA RİSK / ÜST RİSK	RİSK NO	SEBEPLER / KÖK RİSKLER	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	O	E	Ortalama Olasılık	Ortalama Etki	Risk Puanı
Etkin bir Tahsilat Politikaların Yönetilememesi	14	Tahsilatların zamanında ve İstenilen vade de gerçekleştirilememesi	2	3	2	2	2	2	2	2	3	2	3	2	2	3	3	3	2	3	2	3	3	3	2	3	2	2	2	3	2	3	2	3	6
	15	Müşterilerden teminat alınamaması	3	3	4	2	3	2	4	2	3	3	3	2	3	2	3	2	2	3	2	3	3	2	2	3	3	2	2	3	4	1	3	2	6
	16	Müşteri çek/senet vade ertelemeleri (Temdit)	3	3	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	4
	17	Ürünlerin zamanında ve tam olarak gitmemesi	2	2	2	2	2	3	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	4
	18	Piyasa şartlarındaki ekonomik ve sektörel dalgalanmalar	3	3	2	3	3	3	4	2	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	9
Politikaların yazılı hale getirilmemesi	19	Politikaların yazılı hale getirilmemesi	2	2	2	1	2	2	1	1	2	1	1	2	2	2	2	2	2	1	2	1	2	1	1	2	2	1	1	2	2	1	2	1	2
	20	Yetki ve sorumlulukların ve iş süreçlerinin net belli olmaması,	2	2	2	1	2	1	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	1	2	2	4
Stok yönetiminin etkin ve verimli yapılamaması	21	Stokların ekonomik düzeyde gerçekleşmemesi	3	3	2	2	3	3	3	2	3	4	3	3	3	3	2	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	9
	22	Baskı adetlerinin optimum belirlenememesi (ilk ve Ek Baskı)	3	3	3	2	2	2	2	2	2	3	2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	3	2	2	1	2	2	2	4
	23	İade süreçinin etkin ve verimli yönetilememesi	2	2	2	2	4	3	2	2	4	4	3	2	2	3	3	2	3	2	2	3	2	2	2	3	3	2	3	2	2	2	3	2	6
	24	Müfredat değişiklikleri	3	4	3	4	4	3	4	3	4	3	3	4	3	4	3	4	4	3	3	4	3	3	3	4	3	4	3	4	3	3	3	4	12
Mevzuat değişikliklerinin/uyumunun etkin yönetilememesi	25	Yayın hazırlık biriminden ürün çalışmalarının ve üretim süreçindeki gecikmeler	3	4	2	4	3	3	3	3	3	4	3	3	3	3	2	3	4	3	3	4	3	3	2	3	4	3	2	3	3	3	3	3	9
	26	Holding karar verme sürecinin doğru ve hızlı işleyişinin sağlanamaması (İnsiyatif alma/almama, karara alma/almama)	2	3	2	3	2	2	2	2	1	1	2	2	2	2	2	2	2	1	2	2	2	2	1	3	2	2	1	3	1	1	2	2	4
	27	Acil durum senaryolarının bulunmaması	3	3	2	3	4	4	2	3	5	5	4	3	3	4	2	4	4	3	3	4	3	3	4	3	2	3	3	4	3	4	3	4	12
	28	Marka yönetiminin profesyonelce yapılamaması	3	3	2	3	3	3	2	2	1	2	3	2	2	3	2	3	3	3	2	3	2	3	2	3	3	3	3	3	3	2	2	3	6
	29	Eğitim politikalarındaki değişiklik / belirsizlik ve Müfredat değişikliği (MEB)	3	5	3	4	3	5	4	2	4	5	3	4	3	4	3	5	4	4	4	4	4	4	3	5	4	4	4	3	4	4	4	4	16
	30	TTK, Borçlar kanunu ve benzeri düzenlemeler yapılamaması	2	2	2	2	2	3	2	2	2	2	2	3	2	2	2	2	2	2	2	1	1	3	2	3	2	2	2	1	2	1	2	2	4
	31	Gümrük vergisindeki dalgalanmalar	2	1	2	1	1	2	1	1	2	2	2	2	1	1	2	2	1	1	2	2	2	2	2	2	1	1	1	1	1	1	2	1	2
	32	Petrol Fiyatlarındaki ve Döviz kurlarındaki dalgalanma (düşüş) ve Kur tahminlerinin hatalı yapılması	2	2	2	2	2	3	2	1	2	2	3	2	2	2	2	2	2	2	2	2	3	1	2	2	2	2	2	2	1	1	2	2	4

Söz konusu tabloların oluşturulması, diğer bir deyişle, risklerin gerçekleşme olasılığı ile etkilerinin belirlenmesinden sonra yapılacak olan iş, risklerin söz konusu derecelendirmeye göre sırası yine diğer bir deyişle, hangi riskin öncelikle giderilmeye çalışılacak olmasının kararının verilmesidir. Bu amaçla, en yüksek gerçekleşme olasılığı ve en yüksek zarara yol açması beklenen riskler tablonun ilk sırasına konulacak şekilde bir sıralamaya tabi tutulacaktır. Bu sıralama kurum risklerinin yönetilmesinde öncelikle yönetilmesi gereken risklere ilişkin bir fikir edinilmesini sağlayacaktır.

Hangi risklere öncelik verilmesi kararının verilmesinde söz konusu tablonun bir risk haritasına dönüştürülerek risklerin görsel olarak değerlendirilmesi yöneticilere büyük kolaylık sağlayacaktır. Tablo 11 de yer alan verilerin bir olasılık ve etki eksenlerinden oluşan bir haritaya yerleştirilmesi ile söz konusu risk haritasının oluşturulması mümkündür. Dikey eksenin gerçekleşme olasılığı, yatay eksenin oluşabilecek zararı gösterdiği iki eksenli bir haritada yukarıdaki tablonun 2 no'lu sütununda yer alan her bir "alt riskin" olasılık ve etki puanları harita üzerinde bir nokta olarak ifade edilmektedir.

Tablo 11- Risk Haritası

Olasılık					
5					
4				2, 29	
3		15, 23	3, 5, 6, 7, 9, 18, 21, 25	10, 11, 12, 24, 27	
2	19, 31	1, 8, 16, 17, 20, 22, 26, 30, 32	4, 13, 14, 28		
1					
	1	2	3	4	5 Etki

Tablo 11'de yer alan risk haritası kurumun ana ve alt hedeflerine yönelik olası risklerin gerçekleşme olasılığı ve yaratacakları zararları yani etkileri görsel olarak ifade etmektedir, Örneğin 14 no' lu nokta ‘’tahsilatların zamanında ve istenilen vadede gerçekleştirilememe’’ riskinin gerçekleşme olasılığı ve etki bazında risk haritası üzerindeki konumunu ifade etmektedir. Aynı şekilde harita üzerindeki her nokta her bir riskin olasılık ve etki bazında konumlarını ifade etmektedir.

Yine aynı şekilde 23 no’lu nokta ‘’iade süreçlerinin etkin ve verimli yönetilememe’’ riskinin gerçekleşme olasılığı çok yüksek ancak yaratacağı etki çok düşük bir riski, 27 no’lu nokta ‘’acil durum senaryolarının bulunmama’’ riskinin gerçekleşme olasılığı orta ancak yaratacağı etki yüksek bir riski ifade etmektedir.

Risklerin, risk haritaları üzerinde bu şekilde yerleştirilmesi kurumlara hangi risklerinin hem yüksek gerçekleşme olasılığı ve hem de yüksek etkiye sahip olduğunu. Hangi risklerinin yüksek gerçekleşme olasılığı ancak orta veya düşük etkiye sahip olduklarını, hangilerinin ise orta veya düşük gerçekleşme olasılığı ancak yüksek etkiye sahip olduğunu görmelerine yardıma olacaktır.

Son olarak hangi risklerin düşük gerçekleşme olasılığı ve etkiye sahip oldukları da yine aynı harita üzerinden görülebilecektir, Bunun sonucu ise, yüksek gerçekleşme olasılığı ve yüksek etkiye sahip risklerden başlayarak risklerin giderilmesi için uygun alternatifler geliştirilmesi olacaktır.

Tablo 11'te kırmızı bölge ile gösterilen alan en yüksek gerçekleşme olasılığı ve etkiye sahip riskleri ifade etmektedir. Dolayısıyla, öncelikli olarak yönetilmesi veya uygun kontrol önlemleriyle giderilmesi gereken riskler bu riskler olacaktır. Bu risklerin hem gerçekleşme olasılıklarının hem de neden olabilecekleri zararların giderilmesine yönelik bir veya birden fazla kontrol önlemi geliştirilebilecektir.

Sarı bölgedeki riskler, konumlarına göre ya gerçekleşme olasılıkları yada etkileri yüksek riskleri göstermektedir. Sarı bölgede yerleşen alana yakın riskler, gerçekleşme olasılıkları göreceli olarak düşük olmakla birlikte; etkileri giderek artan riskleri ifade etmektedir. Bu riskler için, etkilerini azaltıcı kontrol önlemlerine odaklanılacaktır.

Son olarak; yeşil renk ile gösterilen bölgede yer alan riskler hem gerçekleşme olasılıkları hem de etkileri düşük riskleri ifade etmekte olup söz konusu alandaki

risklere yönelik ilave herhangi bir kontrol önlemi uygulanmasına gerek olmayacak ancak mevcut kontrol önlemlerinin etkinliğinin yeterliliğinin izlenmesi ile yetinilecektir.

Risk haritasıyla birlikte; hem değer korumaya, hem de değer yaratmaya yönelik ana riskler belirlenmiş; farklı senaryolar değerlendirilmiş ve stres testine tabi tutulmuş; içsel ve artık riskler güvenilir bir şekilde değerlendirilmiştir.

Bu aşamadan sonra yapılması gereken öncelikli risklerden başlayarak hangi riske karşı hangi önlemin alınacağının kararlaştırılmasıdır.

4.3.5. Risklere Karşılık Verme

KLM A.Ş. 'nin tüm risklerinin tanımlanması ve değerlendirilmesinden sonra yönetim bu risklerin nasıl giderileceğine dair uygun yöntemler belirlemelidir.

Risklerden Kaçınılması;

KLM A.Ş. nin risklerin kaçınılmasına ilişkin şu öneriler verilebilir;

- İstenmeyen olayların gerçekleşme olasılıklarının kabul edilebilir seviyelere çekilmesi amacıyla risklerin iç süreç veya faaliyetlerle kontrol edilmesi,
- Etkili bir plan dokümanı hazırlanması, karar alma amacıyla uygun kişilerin yetkilendirilmesi yoluyla iyi tanımlanmış acil durum planlarının hazırlanması ve gerekli hallerde uygulanması,
- Riske yol açan olayların büyüklüklerinin azaltılması,
- Yönetim becerilerinin artırılması,
- İyi yönetilemeyen risklerin olduğu yerlerdeki faaliyetlerin risklerin iyi yönetilebildiği alanlara kaydırılması,
- Kurumun iş süreçlerinin, iş modelinin yeniden tasarlanması,
- Kurumun finansal, fiziksel kaynaklarının, müşterilerinin, çalışanlarının, tedarikçilerinin ve kurumsal aktiflerinin çeşitlendirilmesi.

Risklerin Azaltılması;

KLM A.Ş. nin risklerin azaltılmasına ilişkin şu öneriler verilebilir;

- Ürün sayısının çeşitlendirilmesi,
- Operasyonel limitler belirlenmesi
- İşlem süreçlerinin etkinleştirilmesi,
- Karar alma süreçlerine yönetimin daha fazla dahil olması, üst düzey yöneticilerin faaliyetleri izlemesinin etkinleştirilmesi,
- Finansal risklerin yönetimi amacıyla portföy yatırımlarında çeşitliliğe gidilmesi,
- Operasyonel birimler arasında sermayenin yeniden dağıtılması olası risklerin azaltılması çabalarına örnektir.

Risklerin Paylaşılması;

KLM A.Ş. nin risklerin paylaşılmasına ilişkin şu öneriler verilebilir;

- Risklerin iyi planlanmış bir risk yönetimi stratejisiyle bağımsız ve finansal açıdan güçlü bir tarafla maliyet etkin bir yöntemle sigorta edilmesi,
- Sermaye piyasaları işlemleri yoluyla riskin azaltılması, operasyonlarda makul değişikliklerin yapılması veya ilave borçlanma kaynaklarının yaratılması,
- Yeni yatırımlarda yatırımların tamamının kurum tarafından yapılması yerine ortaklarla yapılması,
- Hayati öneme sahip olmayan bazı süreçlerin daha etkin ve az riskli çalışan kurumlara transfer edilmesi,

Risklerin Kabul Edilmesi;

KLM A.Ş. nin risklerin kabul edilmesine ilişkin şu öneriler verilebilir;

- Hiç bir önlem almadan söz konusu riskin olduğu gibi kabul edilmesi ve bu riske rağmen faaliyete devam edilmesi,
- Kurum içi karşılık ayrılması gibi önlemlerle kendi kendine önlemler alınması,

4.3.6. Kontrol Faaliyetleri

Tablo 8 ve 9 da örneği verilen çalışma tabloda yer alan yüzlerce risk için yapılacaktır. Bir risk için birden fazla kontrol önleminin uygulanması mümkündür. Alınacak kontrol önlemleri önleyici, tespit edici veya doğrulayıcı mahiyette olabilecektir. Örneğin, tahsilat biriminde usulsüzlük riskine karşılık tahsilat talebinin yapılması, talebin onaylanması, tedarikçi bilgilerinin bulunduğu tedarikçi ana dosyasının yönetiminden sorumlu olan, siparişi teslim alan, muhasebe kaydını yapan, ödemeyi gerçekleştiren ve banka mutabakatını yapan görevlilerin ayrı kişiler olması bir kontrol önlemi olacaktır. Yine satın almada usulsüzlük riskine karşılık alınabilecek önleyici kontrol önlemlerin den birisi minimum ve maksimum stok seviyelerinin belirlenmesidir. Hatalı tedarikçi seçimine yönelik alınacak kontrol önlemlerinden birisi tedarikçi kriterlerinin ve tedarikçi listesinin üst yönetim tarafından seçilmesidir.

Bu aşamada artık kurumun tüm ana stratejik hedefleri ile alt stratejik hedefleri ortaya konulmuş, bu hedeflerin gerçekleştirilmesini olumsuz etkileyebilecek olası riskler tanımlanmış, söz konusu risklerin gerçekleşme olasılıkları ve yaratabilecekleri zararlar tahmin edilmiş ve en yüksek gerçekleşme olasılığı ve zarar yaratma potansiyeli olan risklere yönelik uygun kontrol önlemleri geliştirilerek uygulamaya konulmuştur.

4.3.7. Bilgi ve İletişim

Bilginin üretilmesi, saklanması, analiz edilmesi ve ilgili yerlere raporlanmasının yanı sıra söz konusu raporlamaların dışında bu bilgilerin içeriğinin kurum içerisinde tartışılması ise iletişim adımının içeriğini oluşturmaktadır.

KLM A.Ş. nin bilgi ve iletişime ilişkin tespitler şunlardır;

- Yönetim riskleri ve bunların nasıl giderileceğini çalışanlarla yaptığı düzenli toplantılarda tartışmaktadır.
- Yönetim kurum çapındaki riskleri çalışanlarla düzenli olarak tartışmaktadır.
- KRY politikaları, standartları ve prosedürleri uyma zorunluluğunun açıkça ifade edildiği bir şekilde tüm çalışanların erişimine hazır tutulmaktadır.
- Yönetim, çalışanların yeni bir risk söz konusu olduğunda tüm kurum çapında diğer çalışanlarla söz konusu yeni riski tartışmasını sağlamaktadır.
- Yeni eleman alımı oryantasyonlarında kurumun risk yönetimi felsefesi ve KRY programı konusunda bilgilendirme seansları yapılmaktadır.
- Kadrolu çalışanların kurumun KRY faaliyetleri hakkında çalışma gruplara katılmaları veya bilgi tazeleyici eğitimler almaları gerekmektedir.
- Kurum kültürünü güçlendirmek için özel iletişim programlan yoluyla ve sürekli devam eden düzenli içsel iletişim programları yoluyla risk yönetim felsefesi güçlendirilmektedir.

4.3.8. Gözlemleme

KLM A.Ş. nin sürekli gözetim faaliyetleri konusundaki önerileri şu öneriler verilebilir.

- Yönetimin önemli faaliyetlere ilişkin yeni satışlar, nakit durumu, finansal kriterler ve operasyonel istatistikler gibi bazı kriterler hakkındaki raporları incelemesi,
- Operasyon birimleri yöneticilerinin üretim, stok yönetimi, kalite kriterleri, satışlar gibi günlük operasyonel faaliyetler sırasında üretilen bilgileri sistemde yer alan veriler veya bütçelerle karşılaştırması,
- Yönetimin kurum performansını kabul edilebilir hata oranlan, bekleyen işlemler, mutabakat bekleyen işlemler gibi gerçekleşen riskleri önceden belirlenen limitlerle karşılaştırması,

- Yönetimin risklerin büyüklüğüne ilişkin trendlerdeki değişimler, stratejik ve taktiksel girişimlerin son durumlarının gözden geçirmesi, gerçekleşen faaliyet sonuçlarındaki değişimleri bütçelerle veya geçmiş dönem sonuçlarıyla karşılaştırması gerekmektedir.

SONUÇ VE DEĞERLENDİRMELER

Küreselleşme ile artan rekabet, değişen ekonomik ve teknolojik koşullar, şirketlerin hedeflerine ulaşmasında, yeni risk faktörleri ile karşılaşmasına neden olmakta veya mevcut risklerini değiştirmektedir. Bu nedenle, küresel rekabet içinde sürekli büyüme ve gelişmeyi hedefleyen şirketlerin, kurumsal risk yönetimine öncelik verdiği görülmektedir. Hem mevcut varlıklarına, hem de gelecekteki büyümelerine yönelik riskleri en etkili ve verimli şekilde yönetmek, uzun vadede yüksek performans sergilemek şirketlerin önceliğini oluşturmaktadır. Bu yaklaşım, riskin kaçınılması değil yönetilmesi gereken bir konu olduğunu göstermektedir.

Risk yönetimi sadece ülkemizde değil uluslararası alanda da henüz gelişme aşamasında olan bir yaklaşımdır. Özellikle son yıllarda uluslararası alanda risk yönetimi kurumsal yönetim stratejilerinin önemli bir unsuru haline gelmektedir. Bütün kuramlarda formel bir risk yönetimi uygulamasının olmasını beklemek doğru olmayacaktır. Ancak bu konuda tüm dünyada çok hızlı bir gelişim yaşanmaktadır. Risk yönetimi konusunda formel düzenlemelere giderek daha fazla yer verilmekte ve kuramların uyması gereken risk yönetimi düzenlemelerinde artış bulunmaktadır.

Risk yönetimi uygulamalarının tüm kurum genelini kapsaması, tüm süreçleri içermesi, risk yönetiminin kurumda çalışan herkesin işi olarak görülmesi, tüm riskleri dikkate alan, birbirlerini nasıl etkileyeceğini irdeleyen senaryoları, risk yönetim strateji ve politikalarının mevcut olması, sadece riskten kaçınmaya odaklanmamış, kuruma değer yaratan riskleri doğru zamanlarda fırsat olarak değerlendirebilen risk yönetim anlayışına sahip bulunulması kurum yönetim kurullarının risk yönetimi konusundaki rol ve sorumluluklarını başarı ile yerine getirebilmelerini sağlamaktadır.

İç denetçiler gerek modern iç denetim uygulamaları gereği, gerekse iç denetim faaliyetleri nedeniyle kurum içerisinde risk kavramının tanıtılması, kurumun faaliyetlerinde karşılaşılabileceği risklerin tanımlanması ve bu risklerin yönetilmesi için nasıl bir sistem kurulması gerektiği konusunda yönetim kurulu ve üst düzey yöneticileri bilgilendirerek kurumsallaşmaya yardımcı olabileceklerdir.

Kurumların kurumsal sürdürülebilirliğinin bir gereği olan bu anlayış yönetim kurullarının öncelikli rol ve sorumlulukları arasına risk yönetimi ve gözetimini dahil etmelerini kaçınılmaz kılmaktadır.

Küresel ve ulusal gelişmeler, yapılan ve yapılmakta olan düzenlemeler çerçevesinde yönetim kurulları risk yönetimi konusundaki rol ve sorumluluklarını başarı ile yerine getirebilmeleri, diğer bir ifadeyle risk zekasına sahip kurum yaratabilmeleri için risk yönetimi ile ilgili strateji, politika ve süreçlerini oluşturulması gerekmektedir.

6102 sayılı Yeni TTK dünyadaki gelişmelere paralel düzenlemeler getirerek Türk işletmelerini daha kurumsal yapıya kavuşturmalarının temel esaslarını belirlemiştir. Özellikle anonim ortaklıkların maruz kaldığı riskleri tespit etme ve bu riskleri asgariye indirme konusunda önlemleri belirleme görevini üstlenerek risk yönetimi ve iç kontrol mekanizmaları oluşturma konusunda yönetim kurullarına görev yüklemiş olması ülkemiz açısından önemli bir gelişmedir. Bu hükümlere uyum sürecinde Anonim Şirketlerin örgütsel yapılarını gözden geçirerek yeni organizasyon şemaları oluşturması, bu yapı içinde yetki ve sorumlulukları uygun şekilde dağıtması etkili iç kontrol ve risk yönetim mekanizmaları kurması gerekmektedir.

Yeni Türk Ticaret Kanunumuzun da risk yönetimi ile ilgili öngördüğü bu yeni uygulamanın, ülkemizin kurumsal yönetim kalitesi, yatırım iklimi ve küresel rekabet gücüne değer katması Anonim Şirketlerin risk yönetimini kurumsallaştırma başarısına bağlı olacaktır.

COSO' nun KRY modeli bu amaca uygun bir model olarak şirketlere önerilmektedir. Aynı paralelde gerek iç kontrolleri, gerek yönetişim süreçlerini, gerekse de Risk Yönetim Sürecinin etkililiğini sürekli izleyen ve değerlendiren bir mekanizma olan iç denetim birimini de oluşturmak gerekli olmaktadır.

Günümüzde kaliteli bir iç denetim fonksiyonu oluşturmak isteyen şirketler Uluslararası İç Denetim Standartlarını referans almaktadır. Tezimizde COSO ' nun KRY modeli ve bu modelin işleyişinde iç denetimin rolü ve sorumlulukları ele alınarak açıklanmış modelin işleyişi somut bir uygulama örneği üzerinde gösterilmiştir.

KAYNAKÇA

KİTAPLAR

CURTİS, Patchin, Mark Carey, **Coso, Rsk Assessment Practice** , October 2012

GRİFFİTHS, Phil. **''Risk-Based Auditing.''** England: Gower Publishing Limited,2005.

GÜREDİN ,Ersin. ''**Denetim''**, 10.Baskı, İstanbul, Beta, 2000,

KAYA, Ertuğrul Bertan, **''İç Denetçi Eğitim Dokümanları,''** İstanbul, 2008,

KENNETH C. Laudon, jane P. Laudon ,**Management Information Systems** 9th Edition 2006

KESKİN, Duygu Anıl, **''İç Kontrol Sistemi Kontrol öz Değerlendirme'',** Beta yayınevi, İstanbul, 2006,

LINDOW,E.Paul , ve D. Race Jill, Beyond Traditional Audit Techniques, **Journal of Accountacy Issues**, July2002,

MCNAMEE, David. ''**Risk Based Auditing.''** CA USA:Management Control Concepts Alamo, 1997.

MOELLER, Robert ''**Brink's Modern Internal Auditing'',** Sixth Edition, New Jersey, John Wiley&Sons, 2005,

ÖZEREN, Baran; iç Denetim, Standartları ve Mesleğin Yeni Açılımlan, Sayıştay, Ankara, 2000.

ÖZBEK ,Çetin, **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol,** TİDE Yayınları İstanbul, Ekim 2012,

PİCKETT ,Spencer **The Internal Auditing Handbook**, 2nd Edition, John Wiley & Sons, 2003,

POLAT, Erdal , **Denetimde Beseri Unsurun Rolü ve Önemi**, Uzman Gözüyle Bankacılık Dergisi, Sayı23,Eylül 1998,

RİTTENBERG, Larry and Frank Martens ,**Enterprise Rısk Management, Understandıng and Communicating Risk Appetite**, January 2012

SAWYER, Lawrence Mortimer D.Dittenhofer, James H.Scheiner,**''Sawyer's Internal Auditing'',** 2003, 5th Edition

SEZEN, Suriye,**'' Kamu Yönetimi Sözlüğü,''** TODAİE Yayınları, Ankara. 1998,

SOBEL, Paul **''Internal Auditing''**,2007

THOMAS, E. Michael **"The Seven-Step Process to Risk-based Auditing",** FSA Times ,Second Quarter,2006 .

UYAR, Süleyman ‘**’İç Kontrol ve İç Denetim 5018 sayılı Kanun Açısından Değerlendirme,’’** Gazi Kitapevi, Ankara, 2009,

URTON, Anderson, “**Assurance and Consulting Services**”, The Institute of Internal Auditors Research Foundation, 2002,

ÜNLÜ, Burak **“Kurumlarda İç Denetimin Değerinin Arttırılması”,** Türkiye İç Denetim Enstitüsü İç Denetim Dergisi, Sayı 9, Sonbahar 2004,

SÜRELİ YAYINLAR VE RAPORLAR

ARSLAN, Işılda **’’Kurumsal Risk Yönetimi’’,** Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Mart 2008,

BORUCU, Ahmet,**’’ Kurumsal Risk Yönetimi Projelerinde Risk Değerleme Sürecinin İşlevi,’’** 2008

CÖMERT,Nuran **’’Denetim,İç Kontrol , İç Denetim Konusunda Dünyada ve Ülkemizdeki Gelişmeler Konusunda Bir Son Durum Değerlendirmesi,’’** III. Türkiye Sektörel Muhasebe Uygulamaları Sempozyumu Panel Notları , Kayseri,

CÖMERT, Nuran ,**’’Sermaye Piyasası Aracı Kurumlarında Etkili Bir İç Kontrol Sistemi ve Denetim Fonksiyonu’’**, Lebib Matbaası, İstanbul 2002,

ÇATIKKAŞ, Özgür, Gürdoğan Yurtsever, **’’Türk Bankacılık Sektöründe Denetim Komitesi Uygulaması’’**, İç Denetim Dergisi, Yaz 2007.

EŞKAZAN, Rıza , “Yeni Yasal Düzenlemeler Işığında İç Denetim”, İç Denetim, Yaz 2005,

Deloitte, ‘’**Risk Zekasına Sahip Kurum,’’** Deloitte Risk Zekası Serisi

Deloitte,**’’ İç Denetim Hizmetleri’’**, Kurumsal Risk Hizmetleri Yayın Broşürü ,

DOĞAN,Mehtap, (çev.), FRASER, John ,Hugh Lindsay**,” Yönetim Kurullarının İç Denetim Hakkında Sorması Gereken 20 Soru”.** (çev.), *IAA Bullettin*

KAYA, H.Abdullah, **“İç Denetim”** Bütçe ve Mali Kontrol Genel Müdürlüğü Maliye Başkanlığı,

MADENDERE, M.Ali **’’Kurumsal Risk Yönetiminde İç Denetimin Rolü,’’** Yayımlanmamış TİDE Döküman,, Ekim 2005,

ÖZSOY,Mehmet Tahir ,**”Risk Odaklı Denetim, ABD Uygulaması ve Türkiye Açısından Değerlendirilmesi”**, Active Dergisi, Mart-Nisan 2009

ÖKSÜZ, Fuat. **”Sabancı Holding’de İç Denetim Uygulamaları”** Türkiye İç Denetim

Enstitüsü İç Denetim Dergisi, Sonbahar-Kış 2005-2006

PİŞKİNOĞLU, Arzu **"Operasyonel Risk Yönetiminde Yaşanan Gelişmeler''**, Active, Kasım -Aralık 2003.

SARENS,Gerrit ve Ignace De Beelde, "Contemporary internal auditing practices: New Roles and Influacing Variables. Evidence from exented case studies", **Working Paper**, (October 2004)

ŞENSOY, Necdet**. "Kurumsal Yönetim Bağlamında Kurumlarda Finansal Raporlama, Kontrol ve Denetim"** Çukurova Üniversitesi Sunum 25 Nisan 2011

TÜSİAD, Risk ve Değer Yönetimi Çalışma Grubu, **''Kurumsal Risk Yönetimi''**, Ankara, 2006

''Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi", Türkiye İç Denetim Enstitüsü Yayınları, No:3, İstanbul, 2005.

Uzun, Ali Kamil; **Türk Ticaret Kanunu Tasarısı ve İç Denetim, İç Denetim Dergisi**, Sayı 16

UZUN, A. Kamil., ''**Aile isletmelerinde Kurumsal Yönetim ve İç denetimin Rolü''**, Deloitte Kurumsal Yönetim Makaleleri

UZUN, A. Kamil., **İç Denetim İle İlgili Düzenleme ve Uygulama Sürecinde Basarı İçin Yol Haritası**

6102 Sayılı Türk Ticaret Kanunu

TEZLER ve İNTERNET KAYNAKLARI

Baydoral, Onur**. İç Kontrol Sistemi Etkinliğinin Muhasebe Denetimindeki Önemi ve Kontrol Riskinin Belirlenmesi.** Yüksek Lisans Tezi Marmara Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2007.

Biçer, Ali. **İç Kontrol Sistemi Etkinliğinini Sağlamada İç Denetimin Rolü ve Bir Uygulama**Yüksek Lisans Tezi Marmara Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2006.

Bilgin, Nil**. Uluslarası Denetim Standartları ve Türkiye Uygulaması** Yüksek Lisans Tezi Marmara Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2006.

Biton, Erika**. Anonim Ortaklıkların Kuruluşu** Doktora Lisans Tezi Marmara Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2006.

Özer, Aptullah. **Risk Odaklı Denetim ve Bir Uygulama** Yüksek Lisans Tezi Marmara Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2008.

Sağlar, Jale **"Bağımsız ve İç Denetimde Kalite Kontrolü: Bağımsız Denetim Firmaları ile Büyük Sanayi İşletmeleri Üzerinde İki Farklı Saha Araştırması",** Doktora Tezi, Adana, 2003, s.115.

Şengür, Evren. **İşletmelerde İç Denetim Fonksiyonu ve Örnek Bir Uygulama**. Yüksek Lisans Tezi İstanbul Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul 2005.

Yenigün, Türkan. **Kurumsal Yönetim ve İşletme İçi Denetim** Yüksek Lisans Tezi Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü. İzmir 2008.

‘’Guide to ERM’’ Protiviti Inc.2006,www.protiviti.com,

www.theiia.org

www.tide.org.tr

http://www.coso.org/documents/COSO-EnhancingBoardOversight_r8_Web-ready%20(2).pdf

http://www.coso.org/documents/ERMUnderstanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

http://www.coso.org/documents/EmbracingERMGettingStartedforWebPostingDec110_000.pdf

http://www.icdenetimmerkezi.com. Risk Yönetim Sisteminin Değerlendirilmesi.

http://www.coso.org/documents/COSOKRIPaperFullFINALforWebPostingDec110_000.pdf

http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf.

http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf

http://kontrol.bumko.gov.tr/TR,2185/coso-hakkinda.html

www.manta.com/mb7refine_company rev=R09&refine cotrıpany_rev)

www.aicpa.org/research/standards/auditattest/asb/downloadabledocuments/clarity/atcpaguide

www.kryd.org