İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ VE TÜRKİYE'DE FARKINDALIĞINA İLİŞKİN BİR UYGULAMA

YÜKSEK LİSANS TEZİ
Şule GÜNEŞ

Anabilim Dalı : İşletme Mühendisliği

Programı : İşletme Mühendisliği

OCAK 2009

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ VE TÜRKİYE'DE FARKINDALIĞINA İLİŞKİN BİR UYGULAMA

YÜKSEK LİSANS TEZİ
Şule GÜNEŞ
(507061027)

Tezin Enstitüye Verildiği Tarih : 29 Aralık 2008
Tezin Savunulduğu Tarih : 20 Ocak 2009

Tez Danışmanları : Prof. Dr. Suat TEKER (OKAN ÜNİ.)
Yrd. Doç. Dr. Mehtap HİSARCIKLILAR (İTÜ)
Diğer Jüri Üyeleri : Prof. Dr. Mehmet TANYAŞ (OKAN ÜNİVERSİTESİ)
Doç. Dr. Oktay TAŞ (İTÜ)

ŞUBAT 2009

ÖNSÖZ

Bu tez çalışmasının hazırlanmasında değerli katkılarından ve desteklerinden dolayı, tez danışmanlarım Sayın Yrd. Doç. Dr. Mehtap HİSARCIKLILAR ve Sayın Prof. Dr. Suat TEKER'e teşekkürlerimi ve saygılarımı sunuyorum. Ayrıca araştırmaya bilgi desteğinde bulunan tüm firmalara da teşekkür eder, hayatım ve tez çalışmam boyunca yanımda olan, beni destekleyenlere ve aileme sevgilerimi ve teşekkürlerimi sunuyorum.

Aralık, 2008

Şule GÜNEŞ
Endüstri Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

ABD	**:** Amerika Birleşik Devletleri
AIRMIC	**:** The Association of Insurance and Risk Managers
ALARM	**:** The National Forum for Risk Management in the Public Sector
BDDK	**:** Bankacılık Düzenleme ve Denetleme Kurumu
CRO	**:** Chief Risk Officer- Risk Yönetim Direktörü
CEO	**:** Chief Executive Officer – Üst Yönetim Direktörü
CFO	**:** Chief Financial Officer- Finansal Yönetim Direktörü
CAO	**:** Chief Audit Officer- Denetim Direktörü
CAS	**:** Causalty Actuarial Society
COSO	**:** The Committee of Sponsoring Organizations of the Treadway Commission
DTY	**:** Değer Temelli Yönetim
ERM	**:** Enterprise Risk Management
ERA	**:** Enterprise Risk Assesment-Kurumsal Risk Değerleme
GAO	**:** Government Accountability Office - ABD Hesap Verilebilirlik Ofisi
IIA	**:** The Institue of Internal Auditors
IRM	**:** The Institute of Risk Management
IT	**:** Information Technology – Bilişim Teknolojisi
KPI	**:** Key Performance Indicators
KSI	**:** Key Success Indicators
KPG	**:** Kritik Performans Göstergeleri
KRG	**:** Krirtik Risk Göstergeleri
KRY	**:** Kurumsal Risk Yönetimi
OECD	**:** Ekonomik İşbirliği ve Kalkınma Örgütü
RIMS	**:** Risk and Insurance Management Society
RY	**:** Risk Yönetimi
SEC	**:** US Securities and Exchange Commission ABD Sermaye Piyasası Kurulu
SOX	**:** Sarbanes Oxley Act
S&P	**:** Standard&Poor's
SPK	**:** Sermaye Piyasası Kurulu
TBS	**:** Treasury Board of Canada Secretariat
TKYD	**:** Türkiye Kurumsal Yönetim Derneği
TTK	**:** Türk Ticaret Kanunu
TÜSİAD	**:** Türk Sanayicileri Ve İş Adamları Derneği
TMS	**:** Türkiye Muhasebe Standartları
TFRS	**:** Türkiye Finansal Raporlama Standartları

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

KURUMSAL RİSK YÖNETİMİ VE TÜRKİYE'DE FARKINDALIĞINA İLİŞKİN BİR UYGULAMA

ÖZET

Risk, iş dünyasının vazgeçilmez bir elementidir ve beklenen getiriden uzaklaşma olasılığı olarak tanımlanabilir.

Dünya çapındaki serbestleşme, liberalleşme, özelleştirme, ticarileşme ve rekabet yapıları gibi reel sektördeki değişim ve gelişmeler ve bunların sistemi etkilemesi nedeniyle belirsizlik ve riskler artmaktadır. Kurumların başarısı büyük ölçüde onların risklerini belirleme, önleme, azaltma ve yönetme kapasitelerine bağlıdır. Kurumsal risk yönetimi bu gerekler için etkin bir yapı sunmaktadır.

Risk yönetiminde muhtelif risklerin konsolide şirketler grubu bazında bütünleştirilmesinin en gerçekçi biçimde yapılması ve yönetilmesi günümüzde geliştirilmesi gerekli en önemli hususdur. Risk ölçümlerinde kullanılan teknik ve yaklaşımlar gittikçe karmaşık ve zor bir nitelik kazanmakta, özel bir ihtisas gerektirmektedir.

Bu çalışmada geniş bir konu olan kurumsal risk ve yönetimi hakkında her işletme için gerekli olabilecek bilgiler verilmiş ve çeşitli risk çeşitleri tanımlanmıştır. Risk yönetimi teorisi ve gerçek durumların kombinasyonu üzerine yerleştirilmiş kurumsal risk yönetimi üzerine teorik ve pratik bir çalışma hazırlanmıştır.

İç denetim özel ve kamu kuruluşlarında uzun zamandır kullanılmaktadır. İç denetim uygulaması dış düzenlemeler (Sarbanes-Oxley Act of 2002 vs.) veya operasyonlarını geliştirmek amaçlı firmalara kendi birimleri tarafından yerleştirilmiş olabilir. Eğer iç denetimde sıcak bir konu varsa bu kurumsal risk yönetimidir.

KRY'de iç denetimin rolünü genişletmeden önce bir düşünce çerçevesi kurmak ve bazı bilgi ve tanımların zeminini sağlamak önemlidir. Tüm bu sebeplerden dolayı bu çalışmada KRY konusu hakkında tanıtıcı bilgiler verilmiş ve ardından Türkiye enerji sektöründeki durum yapılan bir araştırma ile gösterilmiştir.

Anahtar Kelimeler; Kurumsal Risk Yönetimi, İç Denetim

ENTERPRISE RISK MANAGEMENT AND A SURVEY STUDY RELATED ERM AWARENESS IN TURKEY

SUMMARY

Risk is an inevitable element in business world and it could be defined as the possibility of an adverse deviation from a desired outcome which is expected for.

Development and changes in the real sector such as deregulation, liberalization, privatization and commercialization, and competitive structure, uncertainties, risks are increasing and driving due to this developments and changes since these affected the system. The success of an enterprise depends upon its capacity to anticipate, avoid, accept, mitigate and exploit risks. Their survival strongly depends on their ability of managing whole corporate risks. Implementation of enterprise risk management can offer an efficient business framework for these requirements.

Nowadays, the connection of the possible risks in a precise way by the consalidated corporations and the development of the risk management are the most important points. The techniques and the approaches used in determination of the degree of risk are getting complicated and they need specialism.

Though "risk" is a huge topic, in this study, it is tried to give some general information and the main ideas about risk. Also the other types of risk are investigated briefly, since it is thought that every business needs these basics on it.

This study makes a theoretical and practical study on enterprise risk management based on combination of risk management theory and actual case.

Internal audit has been used in enterprises and public institutions management for a long time. Application of internal audit may be implemented by external regulations (e.g. Sarbanes-Oxley Act of 2002 etc.) or by entity itself on the purpose to improve its operations. If there were ever a hot topic in internal auditing, Enterprise Risk Management (ERM) is it.

It is important to establish a frame of reference, and provide some background information and definitions before internal audit's role in ERM can be expanded. For all reasons, in this study descriptive information about ERM is given and then circumstance in Turkey energy sector is represented by an investigation.

Key words; Enterprise risk management, Internal audit

1. GİRİŞ

Globalleşme ve liberal düşüncelerin yaygınlaşması ile birlikte uluslararası piyaslarda sermaye hareketleri çok hızlı bir şekilde gerçekleşmeye başlamıştır. Bunun sonucunda dünyanın herhangi bir ülkesinde ortaya çıkan bir finansal kriz çok hızlı bir şekilde diğer ülkelere yayılabilmektedir. Bu durumdan şirketler etkilenmektedir.

İşletmelerin içinde bulunduğu dinamik ve karmaşık çevrede olayların belirsizlik derecesi ve hızı şimdiye kadar hiç görülmemiş şekilde artmaktadır. Dünyanın en büyük ekonomisi olan ABD'de kredi kriziyle 2008'in son çeyreğinde başlayan sorun finans piyasalarına yansıyınca dalganın boyu da artmaktadır. ABD'de birçok banka bu süreçle birlikte tarihe karışmaya başlamıştır, bu da bazı bankacılık modelleri ile rafa kalkmıştır. Uluslararası finans krizinin neden olduğu bankaların iflas bayraklarını çekmesindeki en önemli etken önlemsizlik ve yetersiz risk yönetimi uygulamasıdır.

Son birkaç yıl içinde, riskleri yönetmede güçlü kurumsal yönetime verilen önem giderek artan bir ölçüde kabul görmüştür. Kurumlar; finansal ve operasyonel risklerinin yanısıra etik, sosyal ve çevresel riskler de dahil olmak üzere, karşı karşıya oldukları tüm iş risklerini tanımlama ve onları makul seviyelerde tutacak şekilde nasıl yönettiklerini açıklama konularında baskı altındadırlar. Bu süreçte, risk yönetimi konusundaki daha az koordine edilmiş yaklaşımlara oranla sağladığı avantajların kurumlarca fark edilmesine bağlı olarak, kurumsal risk yönetimi çerçevelerinin kullanımı yaygınlaşmıştır.

Bilişim teknolojilerindeki gelişmelerin de etkisiyle, 1980'li yıllardan itibaren, ekonomilerin ve toplumların birbirine daha yaklaştığı, dünya ekonomisinin giderek daha bütünleştiği sıklıkla ifade edilmektedir. Küreselleşme olarak adlandırılan bu süreç, değişim hızını, belirsizliği ve karmaşıklığı artırmış, çok büyük fırsatlarla birlikte, ölümcül riskleri de beraberinde getirmiştir. Teknolojideki ve pazar koşullarındaki değişimi kestirebilmek, değişimin içerdiği riskleri fırsatlara dönüştürebilmeyi sağlayacak stratejiler geliştirmek önem kazanmıştır. Küresel rekabet, yeni teknolojilere

ve değişen koşullara hızlı bir şekilde uyum sağlayabilme yeteneğine sahip olmayı gerektirir. Geleceği öngörebilecek, sezgi, hayal gücü ve yaratıcılıkta olmak, riskleri fırsatlara dönüştürebilmek, yönetim yaklaşımlarını etkileyen başlıca faktörlerdir.

Rekabet koşullarına açık sistemler, değişen pazar koşullarından daha fazla etkilenmekte; bu etkileşim, riskleri artırırken risk yönetimini güncel ve kritik bir konu haline getirmiştir.

Bilgi açısından en zengin olduğumuz bir dönemde küresel ekonominin ani değişimlere açık olduğu ve sınırlarının olmadığı bir dünyada yaşamaktayız. Bu yeni düzen içerisinde ulusların ve şirketlerin rekabet gücünün artmasında iş hayatında uygulanan kuralların küresel standartlara uyumlu olması büyük önem taşımaktadır. Artan rekabetle birlikte küresel iş dünyasının değişen gündeminde; şirketlerin büyüme ve gelişme potansiyellerinin değerlendirilmesi, kurumsal yönetim, kamu güveni ve şeffaflık gibi konular öncelikli konuma gelmiştir.

Bu çalışmada amaç; günümüz iş dünyasının önemli gündem maddelerinden biri haline gelen kurumsal risk yönetimi ile ilgili olarak akademik camia ve iş yaşamını bilgilendirmek ve bu konuyla ilgili karşılaşılabilecek temel konuları ve bazı örnekleri paylaşmaktır.

Kurumsal risk yönetimi'ne giriş başlığı altında risk ve kurumsal risk yönetimi kavramları tanıtılacak, kurumsal risk yönetimi çerçevesi, risk yönetimi organizasyonel yapılanma örnekleri ve kurumsal risk yönetimi uygulama yöntemleri anlatılacaktır.

Araştırmadaki teorik bilgiler reel sektöre yönelik olarak hazırlanmış olup, kurumsal risk yönetimi ile ilgili temel bilgileri vermeyi hedeflemektedir. Türkiye'de risk yönetimine genel bakış ile mevcut risk yönetimi uygulamaları ve iç denetim hakkında değerlendirme yapma amaçlanan bu araştırmada enerji sektöründeki büyük ölçekli firmalarda risk yönetim uygulamalarının varlığı ve yapısı araştırılmaktadır.

2. RİSK YÖNETİMİ VE KURUMSAL RİSK YÖNETİMİ

2.1 Risk Nedir ?

Riskin kabul edilmiş tek bir tanımı yoktur. Risk kapsamında kavramsal anlamda farklı ve çok sayıda yorum ve tanım mevcuttur. Genel anlamda risk, bir olayın beklenenden farklı olarak gerçekleşebilme olanağıdır. Risk yönetimi konusunda yeni fikir ve yaklaşımların ortaya çıkışı riskin tanımını daha da genişletmiştir. Risk önceleri tehdit olarak algılanırken yeni bakış açısına göre, "Kurumun hedeflerine ulaşmasına engel olan herhangi bir olay veya durum" olarak tanımlamaktadır (PWC, 2006; RIMS, 2008; Spedding ve Rose, 2007 ve Tevfik, 1997).

Tüm bu tanımlardan çıkarılabilecek ortak tanım şöyle ifade edilebilir: Risk; kurumun hedef ve başarılarını etkileyebilecek, gelecekte olması muhtemel tehdit ve fırsatlardır.

Türk sanayisine uygun yapıda tanımların yer aldığı TÜSİAD (2008a)'ın Kurumsal Risk Yönetimi adlı raporuna göre ise risk; ortalama sonuç olarak risk, sonuçlar arasındaki farklılık olarak risk, kayıp olarak risk, potansiyel kazanç faktörü olarak risk, ilgili oldukları alanlara göre risk olarak kategorizelenerek farklı bakış açılarına sahip, birçok tanımlama ile anlatılmıştır.

Tüm bunlara dayanarak, riskin algıya göre değişebilen çok içerikli bir kavram olduğu söylenebilir.

2.2 Risk Ve Belirsizlik

Belirsizlik riskle yakından ilgili olup, tanımlanması riske eşit derecede zordur. Belirsizlik; sonuçları veya geleceği tanımlayabilme yeteneğimize şüphe ile bakılması olarak tanımlanabilir. Belirsizlik sübjektif bir kavramdır, insandan insana değişir ve bu nedenle de direkt olarak ölçülemez.

Belirsizlik riski kapsamaktadır ve iki boyutu vardır: Birincisi "bilgisizlik" ve ikincisi "sürpriz-şok". Bu anlamları ve boyutlarıyla riskin deney öncesi, belirsizliğin ise deney

sonrası olduğu açıktır. Risk, belli bir tehlikenin gerçekleşmesine ilişkin olasılık hesaplaması yapılarak öngörülebilmektedir ve belli bir maliyet karşılığında, risk altındaki değerin zararına karşı önlem alınabilmektedir. Belirsizlik bu noktada da riskten ayrılmaktadır: Belirsizlik, ancak şok ortaya çıktığında anlam kazanmaktadır. Dolayısıyla, deney sonrası olma özelliği ile belirsizlikte öngörülemezlik ve önlem alınamazlık öne çıkmaktadır (Yalçınkaya, 2004).

Riski yönetmek istendiğinde, daima belirsizliklerle mücadele edilir. Risk gerçekleşebilir veya gerçekleşmeyebilir ki bundan risk meydana gelene kadar emin olunamaz. Risk ortadan kalkana kadar da belirsizlik yok edilemez (Preston ve Guy, 2002).

Risk ve belirsizliği birbirine bağlayan nedenler şöyle ifade edilebilir;

- Risk, belirsizliğin ölçümüdür.
- Belirsizlik yoksa risk de yoktur.
- Gelecek belirsizdir.
- Risk, gelecekte ortaya çıkabilecek olayların dağılımının yaygınlığının ölçümüdür.

2.3 Olasılık ve Değişkenlik

Olasılık, risk değerlendirme tekniklerinin çoğunda kullanılan önemli bir niceleme ölçüsüdür. Olasılık, bir olayın meydana gelme ihtimali ve ifadeler arasındaki mantıksal ilişki olarak tanımlanmıştır. Değişkenlik; hedeflenen/planlanan değerden sapmadır ve riskleri belirleyen temel faktörlerden biridir (Fıkırkoca, 2003).

Birçok risk vakası düzenli aralıklarla ortaya çıkar ve bu nedenle de istatistiksel teknikler kullanılarak etkili bir şekilde modellenebilir. Ancak, olasılık kavramının normal dalgalanmalar dışında ortaya çıkan risklerdeki değeri daha azdır. Bir doğal afet örneği düşünüldüğünde: Olasılık modellemesi genelde bir doğal afetin ne sıklıkta oluşabileceğini gösterebilir (Örneğin her yüzyılda bir kez büyük bir depremin İstanbul'u etkilemesi beklenir). Ama bu modeller hangi yıllarda bu doğal afetlerin olacağını belirtemez ve sonuçları tahmin etme konusunda, birden fazla etken ortaya çıktığında iyi bir iş çıkaramaz (Deloitte, 2008).

2.4 Risk Yönetimi

Riski tarif ederken nasıl bir sürü tanım ile karşılaşılabiliyorsa riski yönetirken de birçok tanım ve yaklaşımla karşılaşılmaktadır. Sözlük terimi olarak risk yönetimi betimlenirse risk yönetimi, "belirsiz olayların etkilerini en aza indirme çabalarıdır" (Güneş, 2006).

Ancak kelime anlamından çok yönetimsel alanda risk yönetimi nedir denilirse; Gartner (2008) "Risk yönetimi, kurumun katlanabileceği kadar risk almasını sağlar. Böylece kurum, olabilecek en yüksek oranda büyüyecektir. Risk yönetimi, iyimser riski maksimize ederken, negatif riski minimize eder." şeklindeki tanımı söylenebilir.

Kurumların en genel hedeflerinin şirketlerine değer katmak ve getirilerini en çoklamak olduğu ışığında, Yüzbaşıoğlu (2003) "Risk yönetimi, *risk* ve *getiri* arasında şirket yönetimine uygun bir geçiş veya değişim yapabilmesini sağlayan bir süreçtir ve risk yönetimi temel bir kurumsal işlevdir" demiştir. Aradaki ilişki şu şekildedir;

Risk yönetimi şirkete "**değer**" kazandırır. Risk almanın karşılığında bir getiri sağlanır getirinin riske oranı ise değeri verir.

Yukarıda verilen tanımlamalarda risk yönetiminin bir süreç olduğundan bahsedilmiştir. Bu süreç, risklerin belirlenmesi, hangi risklerin öncelikli olarak çözümlenmesi gerektiğinin değerlendirilmesi, risklerin yönetilmesi için stratejiler ve planların geliştirilerek uygulanması gibi aşamalardan oluşmaktadır (TÜSİAD, 2008a).

Risk yönetimi tanımları risk yönetimini anlamak için yetersiz gelebilir, bu sebeple risk yönetiminin özellikleri birkaç maddede sıralanmalıdır (Riskactive, 2008; Deloitte, 2001);

- Risk yönetimi mutlaka şirket stratejik kararları ile entegre edilmelidir.
- Risk yönetiminin ortak amaçları şirket çapında belirlenmelidir.
- Risk yönetimi, en iyi hareket planını hazırlamaya yönelik olmalıdır.
- Risk yönetiminin odaklandığı ana konu firmaların maruz kaldıkları ya da üstlendikleri riskleri objektif şekilde ölçerek risk iştahını sınırlandırmaktır Risk

yönetimi, risk/kazanç dengesinin şirket üst yönetiminin risk alma profiline uygun olarak oluşturulmalıdır. Şirketler iktisadi olarak "kâr" elde etmek amacı ile kurulmaktadır. Risk yönetimi, arzu edilen kâr miktarına ulaşabilmek için hangi risklerin, ne ölçüde alınması gerektiğini belirlemeli ve bu sürecin planlanan şekilde gerçekleşmesini güvence altına almayı hedeflemelidir.

- Şirket içindeki herkes risk yönetiminden sorumludur. İşletmelerde risk yönetimi bir takım çalışması niteliğindedir ve çalışanların ortak işidir. Hiç kimse tek başına şirketin tüm risklerinin üstesinden gelebilecek bilgiye sahip değildir.
- Şirkette her kademede yer alan yöneticilerin sorumluluklarının ayrıntılı bir şekilde ortaya çıkarılması gerekir. Tam bir risk şeffaflığı yaratılmalıdır. Ayrıca bu bilincin yanında risk yönetim politikası, risk yönetiminin iş başında eğitimi ile desteklenmelidir.
- Risk yönetiminin başarıyla uygulanmasının anahtarı üst yönetiminin, risk yönetiminin fonksiyonu ve uygulamadaki yararları karşısında bilinçli olmasıdır. Güçlü bir risk organizasyonu kurulmalıdır.

Risk Yönetimi Ne Değildir?

Risk ve yönetiminin tanımını verirken birçok tanımın olduğu söylenmişti. Birçok tanımın olması risk yönetiminin ne olup ne olmadığı konusunda şüpheleri de beraberinde getirmektedir. Bu şüpheleri gidermek için risk yönetiminin ne olmadığını da belirtmekte fayda vardır.

Olasılıkları sıralamak risk yönetimi değildir, önemli olan olasılıklara göre aksiyon almaktır. Risk yönetimi risk almamak değildir, aksine risk almak ve bu riskleri kontrol altına almaktır. Her kurumun maruz kaldığı risklerin farklı olduğu ve kuruma özel risk yönetimi gerekliliği unutulmamalıdır (Riskactive, 2008).

2.5 Risk Yönetiminin Amacı ve Kapsamı

Risk yönetiminin tanımından hareketle amacını, belli bir durumu korumak veya belli bir faaliyeti hedeflenen amaçlar doğrultusunda ve belli bir güvenlikle sürdürmek olarak ifade etmek mümkünüdr. Ayrıca, risk yönetimin amaçları, şirketin yaklaşımını yansıtan

politikalara göre tespit edilmelidir. Bu politikalar sosyal sorumluluğun önemini vurgulamaya çalışıyorsa risk yönetimi bu amaçla yorumlanmalıdır. Benzer şekilde risk yönetiminin örgütlenme şekli işletmede var olan organizasyon yapısı ile aynı olmalıdır (Aksel, 2002).

Risk yönetiminin diğer temel amaçları şu şekilde sıralanabilir (Güneş, 2006):

- Firma yaşamının sürekli kılınması,
- Yöneticilere rahatça düşünme ortamı sağlanması,
- Düşük harcamalara karşı yüksek kazanç sağlanması,
- Gelirde istikrar sağlanması,
- Üretimde yada faaliyetlerde işleyiş kesilmesinin önlenmesi,
- Sürekli büyüme fırsatlarının elde edilmesi,
- Sosyal sorumluluğun yerine getirilmesi, iyi imajın korunması,

Risk yönetimi için şirketlerin politikalara ihtiyaçları vardır. Şirketler ilk iş olarak bu politikaları oluşturmalıdır. Politikalar risk yönetiminin kapsamını açıklamalı ve tüm şirkete bildirilmelidir. Genel olarak risk yönetiminde izlenecek politikalar ;

- Risk yönetimi işlevinin organizasyonu ve kapsamı,
- Risklerin ölçülme usulleri,
- Risk yönetimi grubunun görev ve sorumluluklarının kapsamı,
- Değişik kademelerdeki risk komitelerinin yapıları ve toplanma sıklıkları,
- Risk limitlerinin saptanma usulleri, limit ihlalleri oluşumunda izlenecek yollar,
- Oluşturulacak bildirim ve ihbar usulleri ve işleyiş şekilleri,
- Çeşitli olay ve durumlarda verilmesi zorunlu onay ve teyitler,
- Risk izleme ve kontrolünde kullanılan ölçütler konularını içermelidir.

2.6 Risk Yönetim İhtiyacı

Şirketler risk yönetimine bazı eksiklik ve nedenlerden dolayı ihtiyaç duymuşlardır, sektör ayırt etmeksizin en genel olarak nedenler (Saka, 2006; Uğurel, 2008):

- Kurumun varlığının ve/veya operasyonlarının kesintisiz devam etmesi
- Sürprizlerin en aza indirgenmesi ihtiyacı,
- Artan kriz frekansı ve volatilite,
- Kayıpların maliyetlerinin azaltılması ihtiyacı,
- Gelir istikrarı ihtiyacı,
- Sürdürülebilir büyümeye olan ihtiyaç,
- Sosyal sorumluluğu oluşturma ihtiyacı,
- Yasal düzenlemelere uyum ihtiyacı , olarak sıralanabilir.

Şunu belirtmek gerekir ki risk yönetimi uygulaması, başka koşulların oluşmasına bağlı bir durum değildir. Yönetim şekli ve anlayışı ne olursa olsun, ne tür önemli sorunlar çözüme kavuşturulmamış olursa olsun, başarılı bir yönetim için mutlaka risk yönetiminin uygulanması gerekir. Çünkü kurumun olduğu her yerde, mutlaka riskler vardır ve başka koşulların gerçekleşme şartına bakılmaksızın bu risklerin karşılanması gerekir. Hatta, risk yönetiminin uygulanmıyor olması, çoğu zaman sorunların çözümlenemeyişinin temel nedenini oluşturur (Derici ve diğerleri, 2007).

2.7 Temel Risk Çeşitleri

Riskleri çok genel olarak dahi belli bir sınıflandırmaya tabi tuttuğumuzda birbirinden farklı onlarca riski ortaya koymak mümkündür: Piyasa riskleri, kredi riskleri, faaliyet riskleri, yasal riskler, bilgi riski, çevresel riskler, ülke riski, temel iş ile ilgili riskler, fiyat riskleri, doğal riskler, finansal raporlama riskleri, kontrol riski, v.b.. Her kurum, ihtiyaçlarına uyacak farklı risklere odaklanabilir.

Bu tez kapsamında riskler ana tema olan kurumsal risk yönetimi anlayışına uygun olarak sınıflandırılmıştır. Bu bağlamda reel sektöre yönelik risklere ağırlık verilmiştir.

Kurumsal risk yönetimi kapsamında yapılan bu çalışmada, en kabul görmüş sınıflandırma yöntemi kullanılarak riskler dört ana başlık altında gösterilmiştir:

Finansal Riskler: Finansal riskler kurumun finansal pozisyonunun ve tercihlerinin sonucunda ortaya çıkan riskleri ifade eder. Finansal riskler içerisinde kredi, faiz, nakit, finansal piyasalar, emtia fiyatlarının oluşturduğu riskler lk akla gelenlerdir.

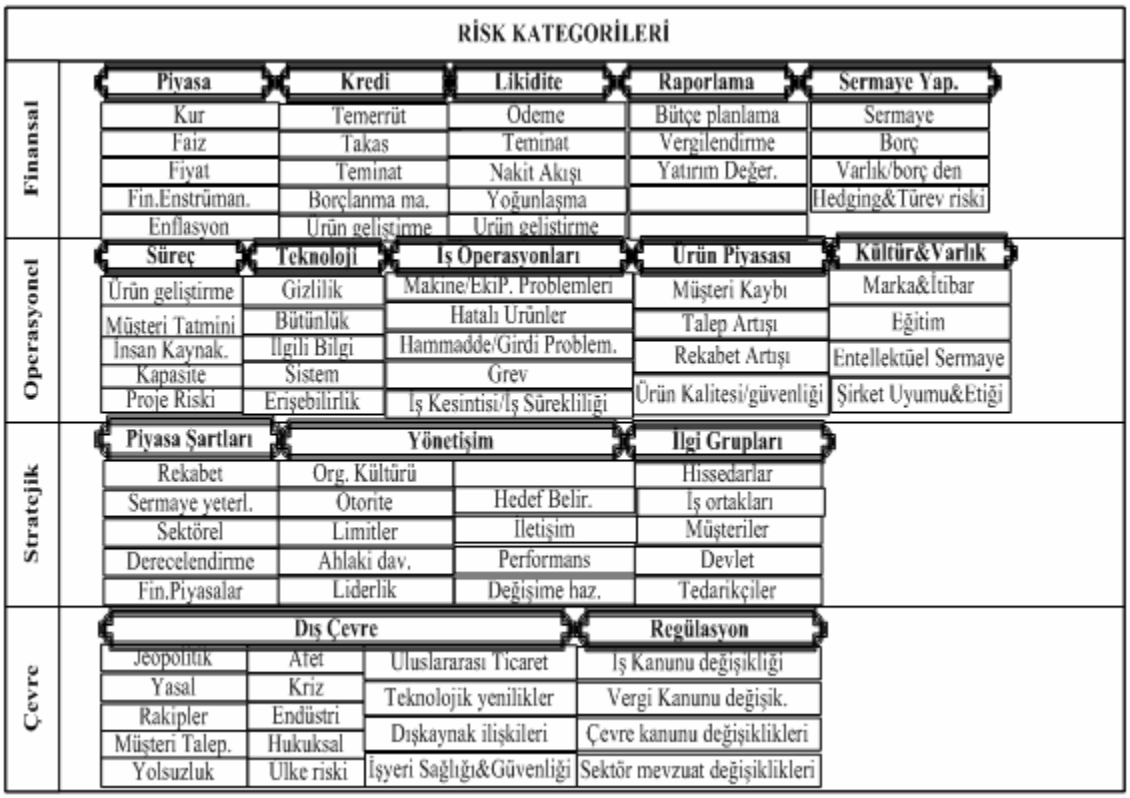
Operasyonel Riskler: Operasyonel riskler bir kurumun temel iş faaliyetlerini yerine getirmesini engelleyebilecek riskleri ifade eder. Tedarik, satış, ürün geliştirme, bilgi yönetimi, hukuk ve marka yönetimi gibi risk başlıkları bu kategori içerisinde yer alan risklerden bazılarıdır.

Stratejik Riskler: Bir kurumun kısa, orta veya uzun vadelerde belirlemiş olduğu hedeflerine ulaşmasını engelleyebilecek yapısal riskler bu başlık altında sınıflandırılabilir. Planlama, iş modeli, iş portföyü, kurumsal yönetim, pazar analizi gibi riskler stratejik risklere tipik örneklerdir.

Çevre Riskleri: Bu kategoride yer alan riskler kurumun faaliyetlerinden bağımsız olarak ortaya çıkan, ancak kurumun tercihlerine bağlı olarak şirketi etkileyen risklerdir. Katastrofik (doğal afet gibi) riskler, yasal düzenlemeler, müşteri trendleri, rakipler, sektördeki değişiklikler, ekonomik ve politik değişiklikler bu kategorideki risklere örnek olabilir.

Bu dört kategorideki riskleri kendi içlerinde de gruplandırarak en sık karşılaşılan risklere Şekil 2.1 de örnekler verilmiştir.

Aslında riskleri kategorilerini kesin çizgiler ile birbirinden ayırmak doğru değildir. Örneğin bir kredi riski; sonuçları itibari ile finansal risk, nedenleri itibari ile de operasyonel bir risk olarak algılanabilir (TÜSİAD, 2008a).



Şekil 2.1 : Risk kategorileri (Kazmirci ve Altunay, 2004; TÜSİAD, 2008a ; Apgar, 2006; Rassumen 2006; Riskactive 2008).

2.8 Risk Kültürü ve Gelişimi

İki bin yıl önce Roma İmparatorluğu'nda yöneticiler kritik kararlar arifesinde kendilerini muhtemel hatalardan korumak amacıyla kahinlere müracat ederlermiş. Bugün ise yöntemler değişmiş olmakla birlikte "gelecekteki belirsizliklerin yol açabileceği zararlardan korunma" çabası öneminden hiçbir şey kaybetmeksizin devam etmektedir. İnsanlığın bu risk yönetimi macerasında en önemli dönemeç, şüphesiz finansal sistemin son yirmi yılda geçirdiği inanılmaz değişim sonunda gelinen noktada ortaya çıkmıştır.

Günümüzde organizasyonlar riski kültürel olarak sistemlerine yerleştirme ihtiyacı duyarlar, bu yüzdendir ki risk esas düşünce halini almıştır. Yöneticilerin organizasyonel büyüme ve kazançlarını artırmak için risklerin avantajlarını alabilme kabiliyetleri olmalıdır; risklerin bilincinde olmak ve risk alabilmek başarılı bir işin büyümesi için asıl gerekliliktir (Collier ve diğerleri, 2007).

Risk konusunda, gelişmiş ekonomilerde, risk yönetimini strateji ve yönetişim ile entegre hale getirmek artık esas hale gelmiştir. Risk algılaması ve risk yönetimi ancak bu şekilde şirketin ayrılmaz bir kültürü haline gelebilmektedir. Bu bir kültür haline gelince de 'risk' şirketler için yalnızca 'önlenilmesi gereken bir öcü' halinden çıkıp 'değerlendirilmesi gereken bir fırsat' haline ve iş yapmanın ruhuna uygun bir 'kâr-zarar' dinamiğine dönüşmektedir (İlkorur, 2008).

2.9 Geleneksel Risk Yönetiminden Kurumsal Risk Yönetimine Geçiş

Risk, önceleri, ayrı ayrı alanlarda yönetilirken günümüzde bu anlayış değişmiş ve risk yönetimi, daha entegre, stratejik, ve kurumsal geniş aktivitelerin olduğu, örgütün bütün seviyelerinde çalışanların dahil edildiği daha sistematik bir yapı halini almıştır.

Yeni bakışlara göre özetle;

Fırsat: Avantaja dönüştürülen ve değer artışa neden olan risk

Belirsizlik: Değişimden dolayı ortaya çıkan risk

Tehlike: Risk yaratan olay, olarak tarif edilmektedir.

Şekil 2.2'de geleneksel risk yönetiminden kurumsal risk yönetimine geçerken nelerin değiştiği gösterilmiştir

Şekil 2.2 : Geleneksel risk yönetiminden kurumsal risk yönetimi'ne geçiş (PWC, 2006; Kazmirci ve Altunay, 2004; Protiviti, 2006a).

1990 yılları boyunca kurumsal yönetimi ile ilgili rehber dokümanların sayısında patlama derecesinde bir artış gözlemlenmiştir. Bu da risk yönetimine olan yatırımı ve ayrılan zamanı artırmıştır. Ancak işletmelerin büyük çoğunluğunda risk yönetimi ayrı bir uygulama olarak ele alınmıştır. Bu nedenle de stratejik amaçlar üzerine risk yönetimi faaliyetlerini odaklama konusunda başarısız olunmuştur.

Hızla değişen ve karmaşıklaşan ekonomik koşullara paralel olarak, mali tablolarda gösterilen kâr zarar ya da firma değeri rakamları (defter değeri), piyasa kapitalizasyonlarıyla birlikte artık bir şey ifade etmemeye başlamış ve dolayısıyla, finansal ve maddi varlıkların korunmasına odaklanan geleneksel risk yönetimi anlayışının yetersizliği ortaya çıkmıştır (Protiviti, 2006a). Bu bağlamda, geleneksel risk yönetimine yöneltilen eleştiriler üç ana tema üzerinde yoğunlaşmıştır.

Bunlar (Sezer, 2005):

- Bütünsel veya koordine bir risk yönetimi anlayışı bulunmamaktadır. Kurum içindeki çeşitli birimler sadece kendileriyle ilgili risklere odaklanmışlardır ve her birim bu risklere özgü tedbirler almışlardır. Kurumun bütününü ilgilendiren önemli riskler bu durumda belirlenememektedir.
- Geleneksel risk yönetimi sadece maddi ve finansal varlıklarla ilgili risklere odaklanır. Müşteri memnuniyetsizliği, çalışanların iş tatminsizliği, tedarikçi riskleri gibi kurumsal amaçlara ulaşılmasına engel teşkil edebilecek riskler üzerinde pek durulmaz.
- Risk yönetimi sigorta şirketleri tarafından satılan bir ürün veya yılda bir defa gerçekleştirilerek daha sonra sonuçları izlenecek bir işlem olarak görülmektedir, Bu anlayış yanlış olup kurum içindeki tüm çalışanların çeşitli roller üstlendiği kurum genelinde uygulanması gereken bir süreçtir.

Yeni anlayışla, firmalar ayrıca hangi risklerin kabul edilebilir ve hangilerinin kabul edilemez olduğuna karar vermek ve riskin daha açık tanımlamasını yapabilmek için ortak bir "risk lisanı" kurmaya başlamışlardır (PWC, 2006).

3. KURUMSAL RİSK YÖNETİMİNE GENEL BAKIŞ

Şekil 3.1 : Kurumsal risk yönetiminde riski sembol eden şekil (Aabo ve diğerleri, 2005).

Kurumsal risk yönetiminde riski simgeleyen anahtar görüş sembolleri Çince'de Şekil 3.1'deki haliyle gösterilmektedir. İlk sembol tehdit, ikinci sembol fırsat anlamına gelmektedir. İkisi birlikte yazıldığında ise risk demektir. Yani fırsat ve tehditin stratejik kombinasyonu risk olarak algılanır (Aabo ve diğerleri, 2005).

Ayrıca bu şekil bir çok risk yöneticisinin odasını süslediği anlamlı bir tablodur.

3.1 Kurumsal Risk Yönetimi Nedir?

Kurumsal risk yönetimi "Enterprise Risk Management"dan Türkçe'ye çevirilse de kimi yönetici bu çevirinin tam da karşılığı olmadığını savunmaktadır. Corporate Risk Management, Integrated Risk Management gibi terimler de Türkçe'ye "Kurumsal Risk Yönetimi" olarak çevirilmiştir. KRY bir kurum fonksiyonundan çok yönetim yetkinliği olarak kabul edilir. Bir kurum mevcut risklerini yönetirken birbirinden tamamen farklı olan iki tür yol izleyebilir. Birincisi mevcut risklerini birer birer ele alıp yönetmek; ikincisi ise tüm risklerini bir spektrumun bir parçası olarak görüp tüm risklerini bir risk yönetimi programı çerçevesinde bütün olarak yönetmektir. İkinci yöntem genel olarak "Kurumsal Risk Yönetimi" olarak adlandırılır.

Kurumsal risk yönetimi için bir çok tanım bulmak mümkündür ama içlerinde en kabul görmüş olanı COSO'nun tanımıdır. IIA (The Institu of Internal Auditors), İnfomag yayınları, CAS (Causalty Actuarial Society), Aabo ve diğ. (2005), TÜSİAD (2008a), kaynaklarında aynı anlayışı benimseyen benzeri tanımlar bulmak mümkündür.

COSO (2004) Treadway Komisyonuna göre en yaygın kabul görmüş tanım şöyledir;

"Kurumsal Risk Yönetimi; şirketi etkileyebilecek potansiyel olayları tanımlamak, riskleri şirketin kurumsal risk alma profiline uygun olarak yönetmek ve şirketin hedeflerine ulaşması, finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ve uygulanabilir yasa ve düzenlemelere uygunluk amaçlarına ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; şirketin yönetim kurulu, yöneticileri ve tüm diğer çalışanları tarafından etkilenen ve iç kontrolü de kapsayarak belirli bir strateji içinde tüm işletme çapında uygulanan sistematik bir süreçtir."

Kurumsal risk yönetimi performans, strateji ve yönetim olarak üç yaklaşımın sentezi olan bir anlayış biçimidir. KRY nin başarı olmasının oturduğu 3 temel taş ve bu 3 temel taşın iyi programlanması olarak da bahsedilebilir. Bu üç temel taş;

Riskin altına giren ve KRY prosesini başlatan, yönetim kurulu, CEO ve CFO'yu da barındıran *yönetim* birinci temel taştır. İkincisi ise risklerin etkilerine maruz kalan *strateji*lerdir. C seviye yönetim (CEO, CFO, CRO…) riskleri değerlendirmeyi, risklerle ilgili seçenekleri belirlemeyi, stratejiyi seçmeyi ve etkinliğini takip etmeyi yönetir.

Üçüncü temel yaklaşım ise *performans*tır. Organizasyonların kâr ve diğer amaçlarını gerçekleştirmek, nakit akışı dalgalanmasını azaltmak, maliyetlerini kontrol etmek, operasyonların politikalarla uyumluluğu ve etkinliğini geliştirmek için performanslarını arttırıcı proseslere ihtiyaçları vardır. KRY performansı arttırmak için bir iskelet sağlar (***Hampton***, 2008).

Entegre Risk Yönetimi Adı Altında Kurumsal Risk Yönetimi

Entegre risk yönetimi, riski kurumsal bakış açısı ile anlayan ve yöneten; proaktif, sistematik ve sürekli uygulayan bir süreçtir. Firmanın, hedeflerine ulaşabilmesi için gerekli stratejik kararları almasında kullanılır (TBS, 2008).

Geleneksel risk yönetiminin yetersizlikleri ve gelecekteki belirsizliklerin somut maddi ve finansal varlıkların ötesinde müşteri tutumu, iş gücü verimliliği, insan kaynakları, işlem süreçleri, müşteri bağlılığı, satıcı riskleri, kurumsal varlıkları ve kültürü gibi maddi olmayan varlıkları da etkilemesi, risk yönetiminin stratejik bir şekilde ele alınarak kurumu ilgilendiren tüm risklerin bütüncül bir şekilde yönetilmesini gerektirmiş ve bu

amaçla ***Entegre Risk Yönetimi*** adı verilen kurumsal risk yönetimi yaklaşımları geliştirilmiştir (Protiviti, 2006).

3.2 Kurumsal Risk Yönetiminin Çerçevesi Ve Kapsamı

Risklerin yönetimi kurum içinde belirli birimlerin ya da ayrı ayrı her bir ünitenin üstlendiği geleneksel risk yönetimi anlayışının aksine KRY yaklaşımı çok daha geniş bir perspektifte ele alır ve kurumsal değerin yaratılması ve korunmasını etkileyen riskler ve fırsatlarla ilgilenir ve tüm işletme çapındaki risklerin stratejik bir şekilde analiz edilmesi ve bir risk profilinin çıkartılması imkanını verir (Thorton, 2003).

Kurumsal risk yönetimi bir bileşenin sırasıyla yalnızca diğer bileşeni etkilediği seri olarak işleyen bir süreç değildir. Her bir bileşenin diğerlerini etkileyebileceği çok yönlü ve dinamik bir süreçtir. Örneğin risklerin değerlendirilmesi risklere verilen karşılığın değişmesine yol açarak kontrol faaliyetlerini etkileyebilir ve sonuçta kurumun bilgi ve iletişim ihtiyaçlarının gözden geçirilmesine, izleme sisteminin yeniden ele alınmasına neden olabilir (Sezer, 2005).

KRY'nde ilk hedef olarak eşzamanlı olabilecek negatif vakaların olasılıklarını azaltmak denebilir belki de ama KRY'nin her şirkette öncelikli hedefleri farklı olabilmektedir (Pagach ve Warr, 2007).

KRY'nin olabilecek hedefleri;

- Olası sürprizlerin belirlenmesi için erken uyarı,
- Sürprizlerin engellenmesi için alınan aksiyonlara danışmanlık,
- Alınan aksiyonların etkin olmasına güvence,
- Tüm faaliyetlerdeki risklerin bir arada görülmesi için raporlama,
- Strateji belirleme, iş geliştirme, kaynak tahsisi, performans takibi fonksiyonlarına destek, olarak sıralanabilir.

Şirket yönetiminin kurumsal risk yönetimi'ne yaklaşımı nasıl olmalıdır sorusunun cevabı arandığında KRY'inin kapsamı ortaya çıkar. Kapsam genişliği bakımından, genel tanımlamayı destekleyici ve genişletici şekilde, KRY'i daha iyi anlamak amacı ile,

aynı zamanda faaliyetleri de sayılabilecek KRY'nin özelliklerinden bahsetmek gerekir (PWC, 2006; Pagach ve Warr, 2007; TÜSİAD,2008a).

Kurumsal risk yönetimi,

- Risk çerçevesi ve ortak risk lisanı sahibi,
- Hem kurum hem de işletme birimlerine tahsis edilmiş personeli olan,
- Risk tanıma, iletişimi ve yönetimini ödüllendiren kültür anlayışı yerleştiren,
- Organizasyonun hedeflerini ileten ve tercüman olan,
- Stratejiyi başarmak için gerekli olan kabul edilmiş risklerin alınmasını, gereksizlerin ise dışlanmasını sağlayan ölçekleri olan,
- Organizasyonlarda ortaya çıkan belirsizlikleri en etkili biçimde yönetme becerilerini geliştiren ve hedefleri başarmak için olası tehditleri belirleyen ve oluşan tehditlerin olasılıklarını ve etkilerini değerlendiren,
- Tek bir olayla veya durumla sınırlı olmayan, zamana yayılı ve organizasyonun kaynağına ve operasyonlarına nüfuz etmiş dinamik bir süreç olan,
- Bir unsurun bir diğerini etkilediği, belli bir sırayı izleyen bir işlem olarak değil, sistematik, tekrarlanabilir ve denetlenen,
- Her seviyedeki çalışanı kapsayan ve risk bakış açısını tüm organizasyona uygulayan,
- Kurumu risk iştahına göre yönetmekte daha hazırlıklı duruma getirirken, risk iştahını ve stratejilerini öncelik sırasına koyan,
- Sermaye rasyonalizasyonuna yardımcı, risk ve kazanç arasındaki bağlantıyı kuran,
- Riske karşın alınan kararların gelişimini destekleyen,
- Operasyonel sürprizlerin ve kayıpların en aza indirilmesine yardımcı olan,
- Çoklu risklere karşı entegre tepkilerin verilmesinin sağlanması ile fırsatların yakalanmasını sağlayan,
- Şirketler arası risklerin belirlenmesi ve yönetimine olanak sağlayan,
- Risk yönetim çerçevesi bulunan uygun bir iç denetim kuran,

- Tüm iş risklerinin etkilerinin proaktif olarak yönetilmesi için uygun mekanizmaların kurulmasını sağlayan,
- Riskin ve değer tabanlı yönetim çerçevesinin esas, ayrılmaz bir parçası olan,
- Üst düzey sahiplik, sorumluluk ve destek isteyen,
- Zorla yaptırmak yerine fikrin pazarlanmasını gerektiren,
- Performans odaklı ve tüm operasyonel iş süreçlerinde etkili,
- Stratejik hedeflerden hareket alan ve strateji belirlenmesi ile entegre,
- Risk yönetim proses ve sonuçlarının koordinasyon ve izlenmesini merkezi olarak sağlamak ve hangi risklerin yönetilmesi ile etkililiğe güvence sağlayan,
- Hissedarın risk alma isteği ile uyumu gözeten,
- Gereksiz bürokrasi oluşturmayan, bir yapıda olmalıdır.

3.3 Kurumsal Risk Yönetiminin Gelişimi

Temel olarak KRY, risk yönetiminin orijinal köklerine dönüşünü temsil etmektedir.

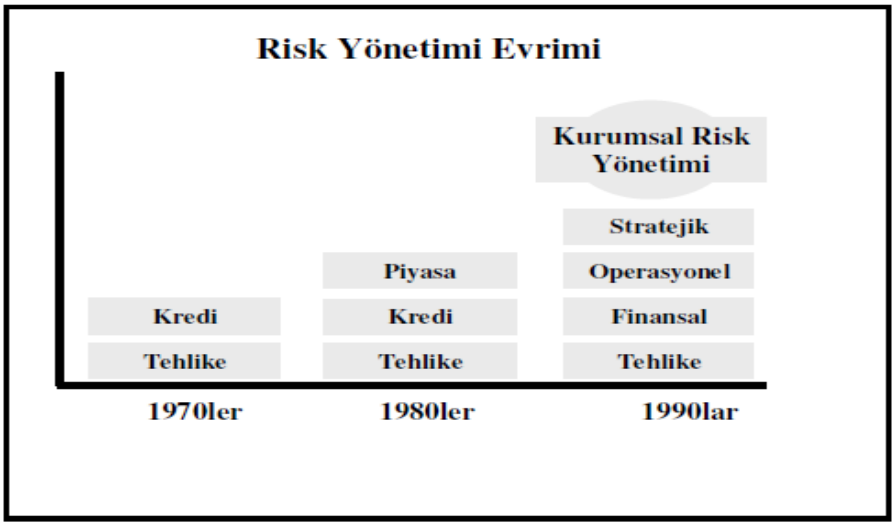
Yirmi yıl önce şirketler için defter değeri, piyasa değerinin belirlenmesinde en önemli faktör iken, günümüzde defter değeri şirketin piyasa değerinin ancak yüzde 20'sini oluşturmaktadır. Geleneksel risk yönetimi ile bu tür gerçek değer yaratan ancak maddi olmayan varlıklara yönelik risklerin yönetilebilmesi mümkün değildir (Sezer, 2005).

Kurumsal risk yönetiminin gelişimi, yönetimin karar verme ihtiyaçları ile ortaya çıkmakta ve piyasadaki risk tanımının değişmesiyle kolaylaşmaktadır. Örneğin, yüksek performanslı şirketler riskin kötü bir olayın gerçekleşebilme olasılığından doğacağı gibi, iyi bir olayın gerçekleşmemesinden de kaynaklanabileceğinin farkına varmışlardır (PWC, 2006).

Kurumsal risk yönetimine ilginin artmasında bir başka faktör KRY yaklaşımını benimseyen şirketlerin performanslarında önemli iyileşmeler yaşanmasıdır (Sezer, 2005). Bu durum, diğer şirketlerin konuya ilgisini artırmış ve entegre risk yönetimi veya

kurumsal risk yönetimi konusunda çeşitli modeller ortaya çıkmıştır. COSO ERM yaklaşımı trendin en son ürünüdür (Kayım, 2006).

Şekil 3.2'de KRY'nin kapsamına dair tarihi gelişim gösterilmektedir. 1970'li yıllarda silo mentalitesi hakimiyetinde sınırlı alanlarda risk yönetimi uygulamaları başlamıştır. 90'lı yıllarda risk yönetimi uygulama alanını finansal ve operasyonel ile genişletmiştir.



Şekil 3.2 : Kurumsal risk yönetiminin tarihsel gelişimi (Shenkir ve Walker, 2002).

Günümüzde gelinen aşamada kurumun karşı karşıya olduğu tüm riskler stratejik, operasyonel, finansal ve tehdit (harici-sigorta edilebilir) risk kategorilerinde toplanmaktadır. Geleneksel risk yönetimi uygulaması olarak silo mentalitesi yaklaşımı ile, tek bir iş birimi veya tek bir seviye hedefi ile ilgili risklerin verilerinin toplanıp analiz edilmektedir. Ancak KRY "portföy" tabanlı ve bütünsel risk bakış açısı üzerinde durmaktadır. Çünkü tek bir risk bütün hedefleri etkileyebilmekte ve birçok hedef de tek bir riskten etkilenebilmektedir. Ayrıca riskler birbirini etkilemekte ve birbirinden etkilenebilmektedir. Riskler arasında çift yönlü bir etkileşim bulunmaktadır. Geleneksel silo yaklaşımında riskler yönetilmeye çalışıldığında işletme yönetiminin elinde birleştirmesi gerekli parçalar olacaktır. Bu parçalar farklı ölçümler, yaklaşımlar sonucu oluşturularak farklı formatta hazırlanacağı için birleştirilmesinde zorluklar ortaya çıkacaktır. KRY'nin amacı bütünsel resmi oluşturmaktır (Küçük, 2007).

3.4 Kurumsal Risk Yönetimine Neden İhtiyaç Duyulur?

Sürekli değişim yaşayan iş dünyası, artan rekabet, ekonomik dalgalanmalar, yasal zorunluluklar, gelişen teknoloji, küreselleşme gibi faktörlerin yarattığı belirsizlikler ile mücadele etmek için etkin iş çözümlerine ihtiyaç duymaya başlamıştır.

Bazı işletmeler bir zorunluluk olarak KRY'e ihtiyaç duymuş bazıları da eksikliklerini kapatma alternatifi olarak ihtiyaçlarını saptamışlardır. ***Hampton*** (2008), "Governance a start for ERM" adlı çalışmasında , yöneticilerin KRY gerekliliğinin sebeplerini beş temele oturttuklarını söylemiş ve şöyle ifade etmiştir;

1. Düzenleyici Mevzuat Zorunlulukları: KRY'yi geliştiren düzenleyicilerdir. Sermaye Piyasası Kurulu kamu kuruluşlarının risk faktörlerinin açıktan açığa tartışıldığı 10-K raporlarını dosyalamalarını gerekli bulmuştur. Basel II de riskler karşısında ellerinde bulundurmaları gereken yeterli sermaye oranını ihtiyaç göstermiştir.

2. Finansal Gereklilikler: KRY borç ve varlık sermayesinin çıkarılmasına da etki eder. New York Borsası risk değerlendirme ve risk yönetimini tartışmak için denetim komiteleri ve şirketler listelemiştir. Derecelendirme kuruluşları da, bir firmanın kredi itibar derecesini başarmadan önce bir KRY programı gerekliliğini ortaya çıkarmaktadır.

3. Saydamlık ve Hesaplanabilirlik: KRY, yönetim prosesini geliştiren önemli bir parça olarak ilerlemektedir. Sarbanes Oxley Act halka açık şirketlerin CEO ve CFO'larının finansal güvenilirlik ve iç kontrollerin yeterliliğini onaylamalarını gerekli kılmıştır. Etkili bir risk yönetiminin proseslerinin yerleştirilmesinin başarısızlığı suç cezasına dahi önderlik edebilmektedir.

4. Rekabet Baskıları: KRY hızla değişen ve çok kompleks çevrelerde faaliyet gösteren organizasyonların risk profillerini geliştirmektedir. Öncelikle, firmaların risk eğilimlerini ve pazarda en başarılı olabilmeleri için bu risklere nasıl karşılık vereceklerini belirlemeleri gerekir.

5. Performans: Birinci önemli şey bir stratejiye sahip olmaktır diğeri ise riskli bir dünyada bu stratejiyi yöneterek ilerlemektir. KRY, yönetimin performansının yüksek seviyede olmasının olasılığını artıran bir araçtır (***Hampton***, 2008).

Bu tez kapsamında KRY'i tetikleyen faktörler iç ve dış etkenler olarak ikiye ayrılmış ve Çizelge 3.1 ve Çizelge 3.2'de gösterilmektedir.

Çizelge 3.1 : Kurumsal risk yönetimi ihtiyacı doğuran dışsal etkenler(Erkan, 2008; Rasmussen, 2006; Saka, Sabancı; Süel, 2001; Uğural, 2008; Vogel , 2006).

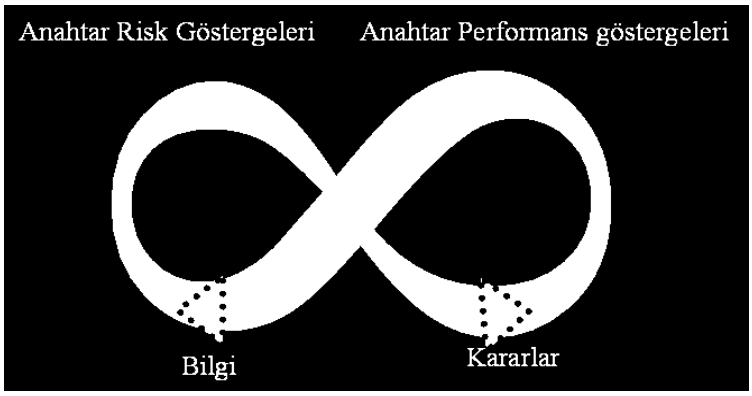
Küreselleşme	Politik istikrarsızlık	Artan rekabet
Müşteri beklentileri	Teknolojik Yenilikler	Doğal afetler
Derecelendirme kuruluşları	Paydaşlar ve yatırımcılar	Pazar çevreleri
Ekonomik belirsizlik	Coğrafi çeşitlilik	Değişen mevzuat/düzenleme
Finans kuruluşlarının beklentileri	Değişen dünya ile artan ve yapısı değişen risk çeşitleri	Artan krizler ve ciddi kayıp olayları
Müşterilerin, satıcıların ve medyanın ilgi ve beklentileri	Örgütlerin uluslar arası platformlarda faaliyet göstermeleri, iş dünyasının değişimi	Yatırımcıların, düzenleyici kurumların,derecelendirme kuruluşlarının, ve sermaye piyasalarının artan ilgileri

Çizelge 3.2 : Kurumsal Risk Yönetimi İhtiyacı Doğuran İçsel Etkenler (Erkan, 2008; Rasmussen, 2006; Saka, Sabancı; Süel, 2001; Uğural, 2008; Vogel , 2006).

Sistem değişiklikleri	Süreçlerdeki değişiklikler	Çalışanlarla ilişkiler
Kurum kültürü	Azalan etik değerler	Yönetim ve yöneticiler
Performans Ölçümü	Risk alma isteği	Hesap verme zorunluluğu
Erken uyarı sistemi iht.	Kurumsallaşma isteği	Daha iyi iç denetim
Çeşitli endüstriler, lokasyonlar, şirketler	Hizmet verilen pazarların çeşitliliği	Risk transfer uygulamalarının genişletilmesi
Hızlı ve doğru karar verebilme ihtiyacı	Organizasyonel değişiklikler	Dağıtılmış operasyonlar ve ilişkiler
Emeğin, çabanın bölünmesi ve çoğalması	Risklerin karşılıklı bağlılıkları	Etik değerlere verilen önem
Hissedarların kontrol fonksiyonuna yetişememeleri	Büyüyen ve karmaşıklaşan şirketlerin farklı risklerle karşı karşıya kalmaları	Finansal performans dışında risk değerlendirmesi ihtiyacı
Karmaşıklaşan ürün ve servisler	Bazı risklerin etkin olarak yönetilememesi, piyasa, çevre ve itibar riski vs.	Riskleri tespit etme, anlama ve risklere hızlı ve kapsamlı cevap verme

3.5 Kurumsal Risk Yönetiminde Kritik Risk Göstergeleri

Kritik performans göstergeleri (KPG), kritik risk göstergelerini (KRG) yürütür. Bu nedenle öncelikle KPG'lerin belirlenmesi gerekir. Aralarındaki bağlantı Şekil 3.3'de gösterilmektedir.



Şekil 3.3 : Performans ve risk göstergeleri arasındaki ilişki (Rassumen, 2006).

Kritik Performans Göstergeleri (KPG)

Ana performans göstergeleri (Key Performance Indicators-KPI) yada Key Success Indicators (KSI) olarak da bilinir. Bir kuruma süreçlerin işletmenin hedefleri doğrultusunda işleyip işlemediğini görmede yardımcı olur. Bir işletme misyonunu analiz edip, hedeflerini ortaya koyduğunda sürecin bu misyon ve hedefler doğrultusunda işleyip işlemediğini ölçme ihtiyacı hisseder. KPG'ler ise bu ölçülerdir ve: iş alanındaki hedefleri yansıtır, başarı için kritik, ölçülebilir ve karşılaştırılabilir ve yanlış giden bir şeyler olduğunda düzeltmeye izin veriyor olmalıdır.

Krirtik Risk Göstergeleri nasıl olmalıdır?

- KRG işin stratejik ölçütlerini içerir.
- KRG işin operasyonel (işlemler, çıktılar, satış rakamları, başarısız işler, operasyonel performans sonuçları, tedarik zinciri/lojistik, vs,) ölçütlerini içerir.
- KRG işin finansal (düzenlemeler, asılsız dengeler, kaçırılmış temrinler, süpheli alacak iptalleri, vs,)ve performans (yüksek risk sonuçları, materyal zayıflığı, süresi geçmiş denetim sonuçları, vs,) ölçütlerini içerir.
- KRG olay ve kayıp ölçütlerini içerir.

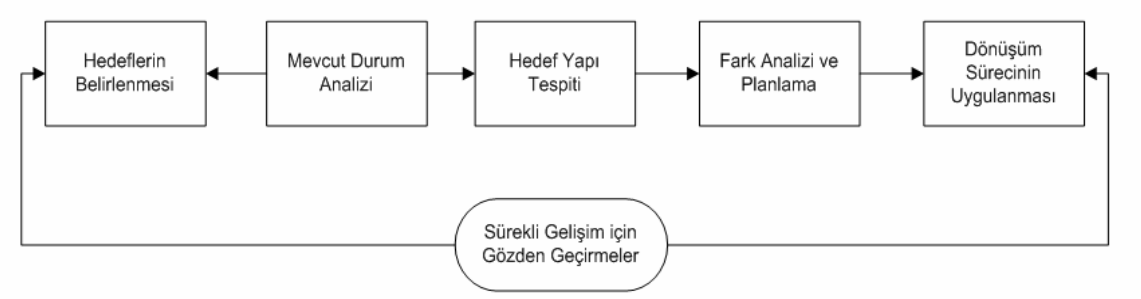
- KRG politika ve uyumluluk (kontrollerin vaziyeti, düzenleyici araştırma/soruşturmalar, hukuki dava durumları, keşif talepleri, şikayetler, vs,) ölçütlerini içerir.

- KRG bilgi teknolojileri ölçütleri; belalar, bozulmalar, zaiyatlar, güvenlik ölçütleri, proje ölçütleri, IT araştırmaları, kazaları, IT denetim konularını içerir.

- KRG insan kaynakları ölçütleri; bordrolu çalışan sayısı, devir hızı, kurumsal eğitim, politikalar, prosedürler, etikler, boş pozisyonlar, hastalık günlerini içerir.

3.6 Kurumsal Risk Yönetimi'nin Kuruma Yerleştirilmesi

KRY dönüşüm süreci, şirketin risklerin birbirlerinden bağımsız bloklar halinde yönetildiği klasik risk yönetim anlayışından, bu risklerin bir bütün olarak yönetildiği entegre risk yönetimi, başka bir ifade ile KRY anlayışına geçiş sürecini ifade eder. Bu süreçte gösterilecek performans başarı için en önemli etkendir. Bu süreç basit bir proje yönetimi anlayışı ile yürütülemeyecek kadar önemli ve karmaşıktır (Sezgin, 2008). Bu süreç Şekil 3.4'de gösterilmektedir.



Şekil 3.4 : Kurumsal risk yönetimi dönüşüm süreci (Tusiad, 2008a).

Hiçbir kurum KRY'yi aynı şekilde uygulamaz ve uygulamamalıdır. Şirketler, KRY becerileri ve ihtiyaçları, bulundukları endüstri ve büyüklükleri, yönetim felsefeleri ve kültürlerine göre büyük oranda farklılıklar gösterir. Bu sebeple bütün kurumlar unsurları yerinde ve etkin bir şekilde işledikleri zaman, şirketin KRY'ni uygulayışı kullanılan yöntemler ve rol ve sorumlulukların tahsis edilmesi dahil olmak üzere çoğu zaman başka bir kurumunkilerden farklı görünür (PWC, 2006).

İdeal bir KRY dönüşüm sürecini aşağıdaki adımlarla anlatmak mümkündür.

3.6.1 Hedeflerin belirlenmesi

Şirket hissedarlarının kurumsal risk alma profillerinin ortak bir anlayışa sahip olabilmesi için öncelikle şirketin genel mevcut konumunu, hedeflerini ve bu hedeflerine nasıl ulaşacağını tanımlayan bir şirket stratejisi ve politikası bulunmalıdır. Stratejiler kadar önemli olan bir diğer unsur ise kurumsal risk alma profilidir. Bu profil kurum hissedarlarının hangi riskleri ne ölçüde almak istediğine cevap arar. Şirketin stratejileri ve kurumsal risk alma profilleri birbirlerinden etkilenen kavramlardır (TÜSİAD, 2008a).

3.6.2. Mevcut durum analizi

Kurum stratejilerinin ve kurumsal risk alma profilinin net bir şekilde anlaşılmasını takiben şirketin mevcut risk yönetim altyapısının ayrıntılı bir şekilde analiz edilmesi gerekmektedir. Bu analiz kurumun karşı karşıya olduğu riskleri, bağımsız olarak bu riskleri yönetmek için var olan sistemleri ve yeterlilikleri kapsamalıdır. Mevcut risk yönetim ortamının değerlenmesinde temel olarak aşağıdaki sorulara cevap aranmalıdır:

- Şirketin risk yönetim anlayışını ve beklentilerini açıklayan yazılı bir "risk yönetim politika (Anayasa)" belgesi mevcut mudur?
- Şirket genel bir "risk alma isteği seviyesi (Risk Appetite)" belirlemiş midir?
- Risk yönetim stratejisi, risk alma isteği seviyesi ve diğer temel risk yönetim politika ve prosedürleri şirket yönetim kurulu tarafından değerlenmiş ve onaylanmış, şirket etik değerleri belirlenmiş, tüm çalışanlara duyurulmuş ve eğitimlerle desteklenmekte midir?
- Kritik pozisyonlar başta olmak üzere tüm pozisyonlar için risk yönetim beklentileri ve gereklilikleri dikkate alınarak yetkinlikler ve yetki/sorumluluklar belirlenmiş midir?

Risk yönetim stratejisi ile ilgili mevcut durum analizinde aşağıdaki soruların cevaplanması uygun olacaktır:

- Şirket fonksiyonlar ve operasyonlar bazında risk toleranslarını belirlemiş midir?
- Şirketin risk yönetim stratejisi ve risk alma isteği seviyesine uygun olarak risk yönetim hedefleri ve bunlara bağlı olarak alınması gereken temel fonksiyonlar açık bir şekilde belirlenmiş ve tüm kuruma duyurulmuş mudur?

Sistematik ve Bütünleşik Risk Yönetim Faaliyetleri ile ilgili sorular ise şöyle olabilir:

- Var olan uygulamalar risklerin belirlenmesi adımlarını yerine getirmekte midir?
- Var olan uygulamalar risklerin değerlemesi adımlarını yerine getirmekte midir?
- Var olan uygulamalar risk yönetim aksiyonları belirlemeyi yerine getirmekte midir?

Kontrol ortamı ile ilgili olarak aşağıdaki temel sorulara cevap aranmalıdır:

- Risk yönetim aksiyonları ile uyum güvence altına alınmış mıdır?
- Kontroller politika ve prosedürler ile belgelenmiş midir?

Bilgi ve iletişim kapsamında değerlendirilmesi gereken soru şudur:

- Şirket içinde risk yönetim faaliyetlerinin etkin bir şekilde yürütülmesini sağlayacak düzeyde bilgi paylaşımı ve iletişim sağlanmakta mıdır?

İzleme ve Sürekli Gelişim ile ilgili sorular ise şunlar olabilir:

- Sürekli izleme faaliyetleri belirlenmiş ve uygulanmakta mıdır?
- Risk yönetim sistemi için bağımsız değerlemeler yaptırılmakta mıdır?
- Risk yönetim sistemi ile ilgili saptanan eksiklikler etkin biçimde raporlanıyor mu?

3.6.2 Hedef yapının tespiti

Mevcut yapının analiz edilmesini takiben yapılması gereken, iyileştirmeler sonrasında erişilmesi arzu edilen hedef yapının belirlenmesidir. Böyle bir analiz yapmaksızın dünyadaki en iyi uygulamaları hedef yapı olarak belirlemek KRY projelerinin başarısızlık ile sonuçlanmasının en önemli nedenlerinden biridir. Hedef yapının belirlenmesinde analiz edilmesi gereken başlıklar aşağıdaki şekilde özetlenebilir:

- Kurumun stratejileri ve hedefleri
- Kurumsal risk alma profili
- Faaliyet gösterilen sektörler
- Faaliyetlerin coğrafi dağılımı
- Faaliyetlerin karmaşıklık düzeyi
- Kurumun büyüklüğü
- Kurum kültürü
- Sektör uygulamaları
- En iyi uygulamalar
- Yasal düzenlemeler
- Menfaat gruplarının yapısı
- İnsan kaynakları (nitelik ve nicelik)
- Kurumun içinde bulunduğu evre (Gelişim, duraklama, küçülme)

Bu süreçlerin birçoğu zaman içerisinde değişebilmektedir. Bu nedenle bu kriterler zaman zaman revize edilerek hedef yapıda gerekli düzeltme ihtiyaçları belirlenmelidir.

3.6.3 Fark analizi ve planlama

Bu aşamada yapılması gereken; mevcut durum ile erişilmesi arzu edilen hedef yapı arasındaki farkın tespiti ve buna uygun olarak detaylı bir aksiyon planının oluşturulmasıdır.

3.6.4 Dönüşüm sürecinin uygulanması

Dönüşüm sürecinde görev ve sorumluluklar bakımından organizasyonel yapı hedef yapıya uygun olarak yeniden düzenlenmelidir. Temel dokümanlar olarak başta politika belgesi olmak üzere standartların, rehberlerin ve uygulama dökümanlarının oluşturulması gereklidir. Bu süreçte, risklerin hangi yöntem ile tanımlanacağı, önceliklendirileceği ve risk yönetim çözümlerinin geliştirileceğinin belirlenmesi ve şirketin tüm çalışanlarının görev ve sorumluluklarına paralel KRY ile ilgili olarak bilgilendirilmesi ve eğitilmesi başarı için kritik öneme sahiptir.

Sistemler ve uygulamalar açısından mevcut durum ile erişilmesi arzu edilen seviye arasındaki farkın giderilmesine yönelik iyileştirici faaliyetlerin, belirlenerek önceliklere uygun olarak gerçekleştirme çalışmaları da gelişim için gereklidir.

Dönüşüm sürecinde herhangi bir aşamayı yanlış veya eksik yapmamak için sürecin devamlı kontrol altında olması ve gelişimi izlenmesi gerekir.

Dönüşüm süreci uygulandıktan sonra firmaya KRY programını entegre etmek gerekliliği ortaya çıkacaktır bu gereklilik için yapılması gerekenler aşağıda proje adımları olarak anlatılmıştır.

3.7 Kurumsal Risk Yönetimi Tesis Edilmesi (İmplemantasyonu)

KRY uygulaması için tek bir doğru yol yoktur. Her kurum uygulamayı kendi ihtiyaçları ve süreçleri doğrultusunda geliştirir. Bazı kurumlar nitel ve bazı kurumlarda nicel yöntemler ve araçlar kullanarak uygulamaya geçebilir (Riskactive, 2008). KRY'nin şirkete tesis edilmesini, yol gösterici olarak, beş adımda özetlemek mümkündür;

1. Adım : Bir kurumsal risk değerlendirmesi (ERA) güdüp, yön vermek

Bu bağlamda iş stratejisi kullanmak, ERA organizasyonun risklerini belirler ve önceliklendirir ve kaliteli girdiler için etkili risk karşılamaların formülasyonunu sağlar, öncelikli risklerin yönetilmesi etrafında yeteneklerin şuanki durumları hakkında bilgileri içerir. Kurumun öncelikli riskleri ile ilişkilendirilmiş açıklıkları belirlemek KRY'nin özgüllüğünün sağlanması için esastır.

2. Adım : Öncelikli riskler çevresindeki açıklıkları kullanan önerme değerlerini ve KRY vizyonunu açıkça beyan etmek.

Anahtar risklerini yönetmek için ihtiyaç duyulan yetenekleri ve organizasyondaki risk yönetimin rolü için KRY vizyonu paylaşılan bir görüş olmalıdır.

Kritik riskleri önceliklendirme ile başlanır ve bu riskleri yönetmek için gerekli yeteneklerin mevcut durumu belirlenir. Birinci adımda anılan ERA'de önceki durumda her anahtar risk için ayrı ayrı değerlendirme yapılır, istenen durum ise açıklıkları amaçlar ile bağdaştırarak belirlemek ve açıklıkları kapatmak için risk yönetim kabiliyetlerinin gelişmesini tavsiye etmektir. Bahsedilen risk yönetim kabiliyetleri veya yetenekleri, politikaları, prosesleri, faaliyetleri, raporları, metodolojileri ve organizasyonun risk karşılamayı sağlaması için gerekli teknolojiyi kapsar. Organizasyonun risk yönetim kabiliyetlerinin olması istenen durumu ile mevcut durumu arasındaki açıklık ne kadar büyükse, o kadar büyük bir altyapıya ihtiyaç duyar.

3. Adım : Bir veya iki öncelikli risk için organizasyonun risk yönetim yeteneklerini ilerletmek

Sarbanes-oxley 'in 404 ve 302inci maddeleri, kurumsal risk değerlendirme esaslı bir veya iki öncelikli finansal veya operasyonel risk düzenleyici uyum riskleri veya yönetim reform konuları ve KRY'nin yönetim prosesleri ile entegrasyonu gibi KRY'nin başlamasını gerekli hale getiren başlangıç noktaları vardır. Bu başlangıç noktalarından hangisinin başlamaya sebep olacağı belirlenir.

4. Adım : Var olan KRY altyapısının değerlendirilmesi ve gelişmesi için bir strateji oluşturmak.

KRY altyapısı kurulumu üç önemli şeyi kolaylaştırır. Birincisi kurumun riskleri ve risk yönetim kabiliyetlerini anlamaya yönelik yapıyı kurar. İkincisi, kritik riskler üzerinde mülkiyetin var olmasını sağlar. Sonuncusu ise, kabul edilemeyecek açıklıkların kapatılmasını sağlar. KRY altyapısı her yere, her kurumu, her duruma uygun bir yapı değildir. Bir kurum için çalışabilirken diğeri için çalışmayabilir. KRY altyapısının elementleri, KRY kurulumu için konuşlandırılmış teknik ve araçlara, örgütün kültürüne, belirlenmiş hedeflerin genişliğine ve örgütün işletim birimlerinin kapsam genişliğine göre çeşitlilik gösterir. Yönetim bunlar ve diğer uygun faktörlere göre KRY altyapısının elementlerine karar vermelidir.

5. Adım : Diğer anahtar riskler için risk yönetim kabiliyetlerini geliştirmek.

İlk dört adım tamamlandıktan sonra, yapılması gereken ERA (kurumsal risk değerlendirme) 'nin güncellenmesidir. Bu adımda, yönetim kurumun odaklanacağı öncelikli riskleri genişletir (Protiviti, 2006).

Risk yönetiminin etkili ve sürdürülebilir olması için işin günlük operasyonlarına gerçekten de yerleştirilmesi gerekir. Birçok organizasyon açısından risk yönetiminin en zorlu kısmı sistemin etkin olarak benimsenmesini sağlamaktır.

KRY'nin şirkete tamamen yerleştirilmesi için aşağıda üç aşamada görevler ve bu görevler ile gerekli belgeler belirtilmiştir.

1. Çevresel tarama, projeye başlama vuruşu ve farkındalık oluşturma

Risk değerlendirme aktiviteleri, yaklaşımı, geçmişi ve düzenleyici raporlar ile bilgi toplama ile başlayan görevler proje planını, zamanlamasını ve anahtar çıktılar üzerinde anlaşmayı geliştirme ile devam eder. Risk yönetim komitesinin ve üst yöneticinin risk farkındalığı, eğitim ve materyallere inanmasını geliştirmek ile şirkette senyor yönetici ile görüşmeleri başlatmak ve çizelgelemek, proje planını ve çıktılarını yönetimle birlikte geçerliliğini onaylamak, bir risk dili belirlemek, kayıtlı risk anketi geliştirmek ve bu anketleri iş birimlerinde cevaplayacak kişileri belirlemek bu aşamanın en önemli görevlerindendir. Bu bölümde oluşturulması gereken belgeler; proje planı dökümanları**,** risk farkındalığı oturumlarının slayt ve materyalleri, şirketin risk dünyası ve görüşmeleri yürütmede kullanmak ve iş birimlerine dağıtmak için risk anketleridir.

2. Risk değerlendirme çalışmalarını yürütme

Şirketin yönetici üyeleri ile risk değerlendirme görüşmelerini yürütmek ve görüşmelerin sonuçlarını derlemek, Kritik risk ve stratejileri belirleme, analiz ve önceliklendirme için risk değerlendirme üzere kolaylaştırılmış çalışmaları yönetmek, İş birimleri için bir risk değerlendirme tetkiki taksim etmek ve geliştirmek, Tüm iş birimleri için risk değerlendirmelerin ve tetkiklerin sonuçlarını analiz etmek ve derlemek bu bölümün görevlerindendir.

3. KRY için yüksek seviyede çalışma planını ve raporlamayı geliştirme

Her bir birim için anahtar riskleri önceliklendirme için risk haritaları geliştirmek, holding için genel bir risk haritası oluşturmak, top on iş riskleri için risk yönetim stratejilerinin vadelerini değerlendirme, bir ayrım çözümleme (gap analysis) hazırlamak ve top on anahtar iş riski için risk yönetimini geliştirmeye yönelik amaçları belirlemek, risk yönetim kabiliyetlerini geliştirmek için, yüksek seviye bir KRY kurulum planı belirlemek, yönetim ve kurul arasında iletişim stratejilerini içeren uzun dönem KRY planının kurulumunu sonuçlandırmak ve final raporu hazırlayıp, gözden geçirmek ve teslim etmek görevleri tamamlandığında KRY şirkete tamamen yerleşik duruma gelmiş demektir. Her birim için anahtar riskleri önceliklendirme ve özetleme için risk haritaları ve holding çapında genel risk haritaları bu bölümün gerekli belgelerindendir.

3.8 Kurumsal Risk Yönetimine İlişkin Roller ve Sorumluluk

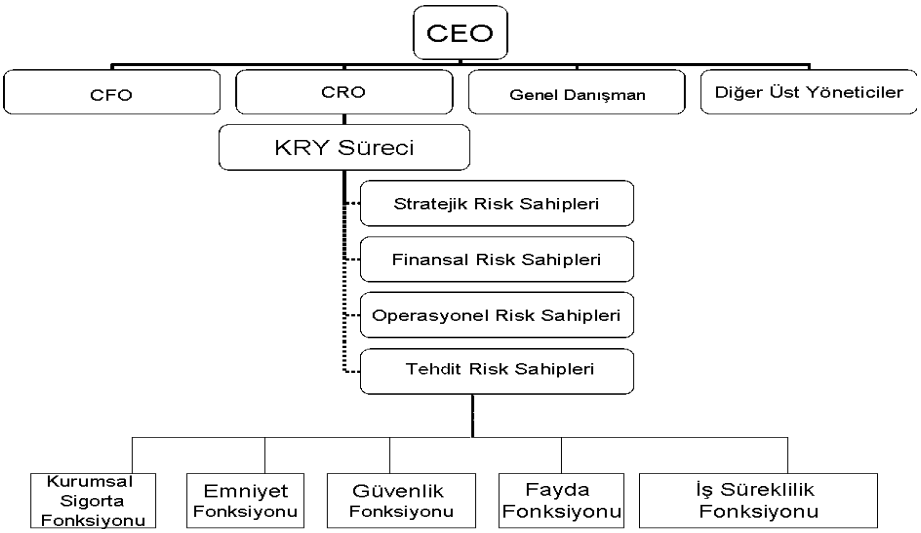
Bir kurumun organizasyonel yapısı planlama, uygulama, kontrol ve izleme faaliyetleri için çerçeve oluşturur. Uygun bir organizasyon yapısı yetki ve sorumluluk gibi önemli alanları tanımlamayı ve uygun raporlamanın yerleştirilmesini içerir (Küçük, 2007). Etkin bir risk yönetiminde her bir çalışanın rolü olmakla birlikte, risklerin tanımlanması, yönetimi ve kurumsal risk yönetiminin sistematik, tutarlı ve koordineli bir şekilde yürütülmesinde asıl sorumluluk yönetime aittir (IIA, 2004). Yönetim kurulunun temel yükümlülüklerinden biri, risk yönetimi süreçlerinin etkili biçimde işlediği ve temel önemli risklerin yönetilerek makul seviyelerde tutulduğu konusunda güvence elde etmektir (Madendere, 2005). Ayrıca risk iştahını belirleme ve üst yönetimin performansını izlenme de yönetim kurulunun en temel görevlerindendir.

KRY'nin parçalarına bakıldığında finansal yöneticilerin ve çalışanlarının da çok önemli pozisyonda bulundukları görülür. Finansal yöneticiler hedeflerin oluşturulmasında, stratejilerin belirlenmesinde, risklerin analiz edilmesinde ve kurumu etkileyen değişikliklerin nasıl yönetileceği konusunda karar verilmesinde, vazgeçilmez bir görev taşır, çok değerli bilgiler sağlar, yön gösterir ve karar verilen aksiyonların izlenmesi ve takip edilmesi sağlayacak bir pozisyonda bulunur (Lam, 2003).

Yönetim bir kurumun, KRY dahil tüm faaliyetlerinden direkt olarak sorumludur. Doğal olarak farklı yönetim seviyelerinin farklı KRY sorumlulukları vardır. Bunlar çoğu zaman kurumun özelliklerine göre değişir. Herhangi bir kurumda, KRY'nin nihai sorumluluğu CEO'lardadır. Bu sorumluluğun en önemli parçalarından biri olumlu bir iç ortamın yaratılmasını sağlamaktır. Bir CEO ayrıca, yönetim kurulunun yeni üyelerinin belirlenmesinde, üye adaylarına örnek oluşturmada yönetim kurulunu etkileyebilir. CEO, üst düzey yöneticilerle birlikte, kurumun KRY'sinin temellerini oluşturacak değerleri, prensipleri ve önemli işleyiş kurallarını biçimlendirir (Küçük, 2007).

Uygulamada, yönetim kurulu, risk yönetimini üst yönetime bırakmakta ve üst yönetim risk yönetimine ilişkin faaliyetleri icra etmektedir. Ayrıca kimi şirketlerde, söz konusu risk yönetimi aktivitelerinin koordinasyonu ve idaresi ayrı birimlerce yürütülmektedir (Matyjewicz ve D'arcangelo, 2004). CRO, risk birimi yöneticisi veya risk idarecisi, risk başkanı olarak anılmaktadır, etkili KRY tesis edilmesinde ve uygulanmasında diğer yöneticiler ile birlikte çalışır. CRO, sürecin izlenmesinde ve kurumun yukarı, aşağı ve çapraz risk ile ilgili bilgilerinin raporlanmasında diğer yöneticileri desteklemek, onlara yardımcı olmakla sorumlu olabilir. Bazı işletmeler bu rolü, bir başka üst yönetici, örneğin CFO, genel danışman, CAO veya atadığı bir başka yöneticiye vermektedir. Diğer işletmeler ise, bu fonksiyonu daha önemli ve geniş kapsamlı ele alarak, gerekli ayrı atamaları yaparak ve kaynaklar tahsis ederek gerçekleştirmektedir. CRO riskin tüm yönlerini içeren KRY stratejisi geliştirmek ve uygulamaktan sorumlu olduğu gibi genel olarak risk politikası, sermaye yönetimi, risk analitiği ve raporlamadan sorumludur ve iş birimlerinde risk yönetiminin başıdır. Çünkü CRO, KRY uygulamalarında tecrübeleri ve gerekli altyapıyı oluşturması kapsamında da yararlıdır (Lam, 2003).

Yapılanması nasıl olursa olsun, kurumlar etkili bir KRY'ye ve kurumun hedeflerine ulaşmasını sağlayacak faaliyetleri yapmasına olanak sağlayacak bir şekilde organize olmalıdır. En modern ve yalın haliyle organizasyon şeması Şekil 3.5'deki gibi olabilir.



Şekil 3.5 : Modern risk yönetimi modelinde organizasyon yapısı (RIMS, 2008).

İç denetçiler KRY'nin etkinliğinin değerlendirilmesi ve düzeltmelerin önerilmesinde aktif rol oynarlar. Yerel yada uluslararası enstitüler tarafından oluşturulan standartlar iç denetimin risk yönetimi ve kontrol sistemlerini de içermesini gerektiğini vurgular. Böylece, raporlamanın güvenilirliği, operasyonların verimliliği ile yasa ve düzenlemelere uygunluğunu değerlendirmesini de içerir. İç denetçilerin ayrıntılı görev ve sorumlulukları İç denetim ve KRY İlişkisi bölümünde açıklanacaktır.

KRY, bir düzeye kadar, kurumdaki herkesin sorumluluğundadır ve dolayısıyla herkesin iş tanımının bir şekilde parçası olmalıdır. KRY, görev ayrımını içeren kontrol noktalarına ve dengelere ayrıca gördüklerini söyleyen çalışanlara dayanır. Çalışanlar, üstlerinden gelebilecek uygunsuz hareketlerde bulunma baskısına karşı koymanın gerekliliğini anlamalı ve bu gibi durumları raporlayarak, normal raporlama sıralamasına alternatif iletişim kanalları oluşturulmalıdır. (Küçük, 2007).

Tüm bu mercilerin dışında işletmeler dışardan da desteğe ihtiyaç duyabilirler. Üçüncü kişiler olarak adlandırdığım kurum dışı kişiler kapsamında dış denetçiler, yasa koyucular ve düzenleyiciler, kurum ile etkileşimli kişiler, dış kaynak hizmet sağlayıcıları, finansal analistler ve tahvil derecelendirme kuruluşları yer almaktadır.

4. KURUMSAL RİSK YÖNETİM SÜRECİ ve BİLEŞENLERİ

Risk Yönetim süreci;

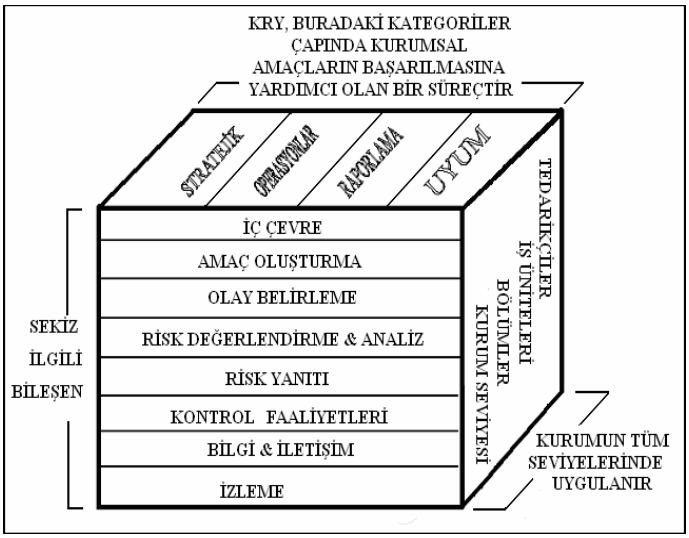
- Anahtar prosesleri ve içerdiği proses adımlarını belirleme,
- Türlerine göre adımları sınıflandırma veya bir risk sınıfına göre özelleştirme,
- Modelleme ve takip etme ie spesifik bir risk sınıfı oluşturmadır.

KRY süreci ile aşağıdaki beş temel soruya daha doğru ve etkin cevapların bulunmasına destek olunması amaçlanmaktadır (TÜSİAD, 2008a):

- Risklerin neler olduğu gerçekten biliniyormu?
- Bu riskleri faal bir şekilde yöneterek, risk/kazanç dengesi lehde kullanılabiliyormu?
- Riskler için uygun kontroller var mı? Kontroller etkili bir biçimde çalışıyormu?
- Hangi kontroller iyileştirilmek/geliştirilmek zorundadır?

4.1 Kurumsal Risk Yönetimi Yapısında Amaçların ve Bileşenlerin İlişkisi

KRY yapısında yer alan amaçlar kurumun başarmaya çalıştıkları olup, KRY aşamaları ile arasında direkt bir ilişki vardır. KRY aşamaları, amaçları başarmak için ihtiyaç duyulan unsurları göstermektedir. Bu ilişki üç boyutlu bir matris ile Şekil 4.1'de gösterilmektedir (COSO, 2006).



Şekil 4.1 : Kurumsal risk yönetiminde amaç ve bileşenlerin ilişkisi (COSO, 2006).

KRY yapısının etkin ve etkili şekilde uygulanabilmesi, potansiyel faydalarının gerçekleştirilmesi için önemlidir. Kurumda KRY uygulanması için örnek yapılar rehber olarak kabul edildiğinde öncelikli olarak yapılması gereken örnek KRY yapılarının kurumun geliştirdiği yapı ile bütünleştirilmesinin sağlanmasıdır. Bu amaçla kurum ilk olarak kendi KRY yapısının altyapısı ve süreçlerini oluşturur. Ardından örnek KRY yapıları ile kendi KRY yapısını kıyaslar ve sonra bütünleştirir (Küçük, 2007).

Trendin en son ürünü olan "COSO-ERM" çok kabul görmüş bir çerçevedir, çoğu şirket bu çerçeveyi kabul edip içlerini kendileri kurumlarına özgü doldurmaktadır.

COSO-ERM risk yönetimi, iç denetimin etkinliği ve tarafsızlığı gibi konularda kurumlara kaynak teşkil etmekte olup iç denetim organları tarafından yol haritası olarak kabul görmektedir. COSO iç kontrolü birbiriyle ilişkili sekiz unsurla tanımlayan entegre bir çerçeve sunar. Yatay eksende dört amaç kategorisi gösterilmektedir ki bunlar; strateji, operasyonlar, raporlama ve uyum'dur. Dikey eksende süreci oluşturan sekiz aşama bileşeni, kurum seviyeleri ise matrisin üçüncü boyutunda gösterilmektedir.

i) Kurumsal Çevre: Diğer tüm bileşenlerin temelini teşkil eder ve kurumun strateji ve hedeflerini nasıl belirlendiğini, faaliyetlerin nasıl yapılandırıldığını, risklerin tanımlanmasını, değerlendirilmesini ve risklerle ilgili alınan tedbirlerin uygulanmasını etkiler. Kurumun risk kültürünü kurar. Kurumun etik değerleri, çalışanların yetkinliğine verilen önem, yönetimin çalışma biçimi, görevlerin ve sorumlulukların dağılımı vb bir çok faktörü bünyesinde barındırır.

ii) Hedef Belirleme: Kurumsal risk yönetiminin söz konusu olabilmesi için öncelikle yönetim tarafından operasyonel, raporlama ve uygunluk amaçlarını da kapsayacak şekilde hedeflerin belirlenmesi gerekir. Hedefler ayarlanırken, yönetim risk stratejisini dikkate aldığı zaman başvurulur. Kurumun, yönetimin ne ölçüde riskleri kabul edebileceğini simgeleyen risk iştahını şekillendirir. Hedeflerin kabul edilebilir bir varyansı olan risk toleransı , risk iştahı ile sıralanır.

iii) Gerçekleşmesi Muhtemel Olayları Belirleme ve Tanımlanması: Yönetim, kurumsal stratejilerin uygulanmasını, amaçlara ve performans hedeflerine ulaşılmasını etkileyebilecek muhtemel olayların neler olduğunu belirlemelidir. Risk ve fırsatları ayırır. Olayın negatif bir etkisi var ise, riski tasvir eder, eğer pozitif bir etkisi var ise

fırsatı tasvir eder. Başarı ve strateji hedeflerine etki edebilecek olayları içsel kaynaklı mı dışsal kaynaklı mı olduğunu belirler.

iv) Risk değerlendirme: Kuruma hedefleri etkileyebilecek olayların hangileri olduğunu anlama imkanı sağlar. Risk değerlendirme riskleri değerlendirmede ve ilgili hedefleri ölçmekte kullanılır. Kalitatif ve kantitatif risk değerlendirme metodolojilerinin bir kombinasyonudur. Riskler *"etki ve olasılık"* olarak iki şeye göre değerlendirilir.

v) Risk Tepkisi: Risklere verilebilecek cevapları belirler ve değerlendirir. Bu cevaplama kurumun risk iştahına ve risk karşılamadan olabilecek yarar ve maliyetine göre,olasılık ve/veya etkiyi azaltabilecek seviyeye göre seçenekleri değerlendirir.Risk portföylerini ve risk karşılamanın üzerine değerlendirilmiş cevapları seçer ve yönetir. Bu bağlamda, risklere verilebilecek tepki dört şekilde olabilir: Bunlar;

Riskten Kaçınma : Riske neden faaliyetlerden vazgeçmektir. Bir ürünün üretiminden vazgeçmek, bir bölgedeki genişlemeyi durdurmak veya bir bölümü satmak gibi olabilir.

Riski Azaltma : Riskin gerçekleşme olasılığını veya riskin gerçekleşmesi durumunda etkilerini azaltmak için ortaya konan faaliyetleri kapsamaktadır.

Riski Paylaşma : Riskin gerçekleşme olasılığını veya riskin gerçekleşmesi durumunda etkilerini azaltmak için riski transfer etmek veya riskin bir kısmını bir başka tarafla paylaşmaktır. Riski paylaşma yöntemleri olarak en çok görülenler: sigorta yapılması, risk havuzları oluşturulması, kurumun içinde gerçekleştirilen kimi hizmetlerin veya üretilen ürünlerin dışardan alınmasıdır.

Riski Kabul Etme : Karşılaşılan riskle ilgili olarak gerek riskin gerçekleşme olasılığı ve gerekse de riskin gerçekleşmesi durumunda etkilerine bir şey yapılmamasıdır.

vi) Kontrol Faaliyetleri: Risklere verilen cevapların hayata geçirilmesine ve kurum direktiflerine yardım sağlayacak risk politika ve prosedür faaliyetleridir. Bütün fonksiyonlarda örgütün bütün seviyelerinde baştan başa tüm örgütte vuku bulur. Teknololjik kontrolün genel bilgisi ve uygulamasını içerir.

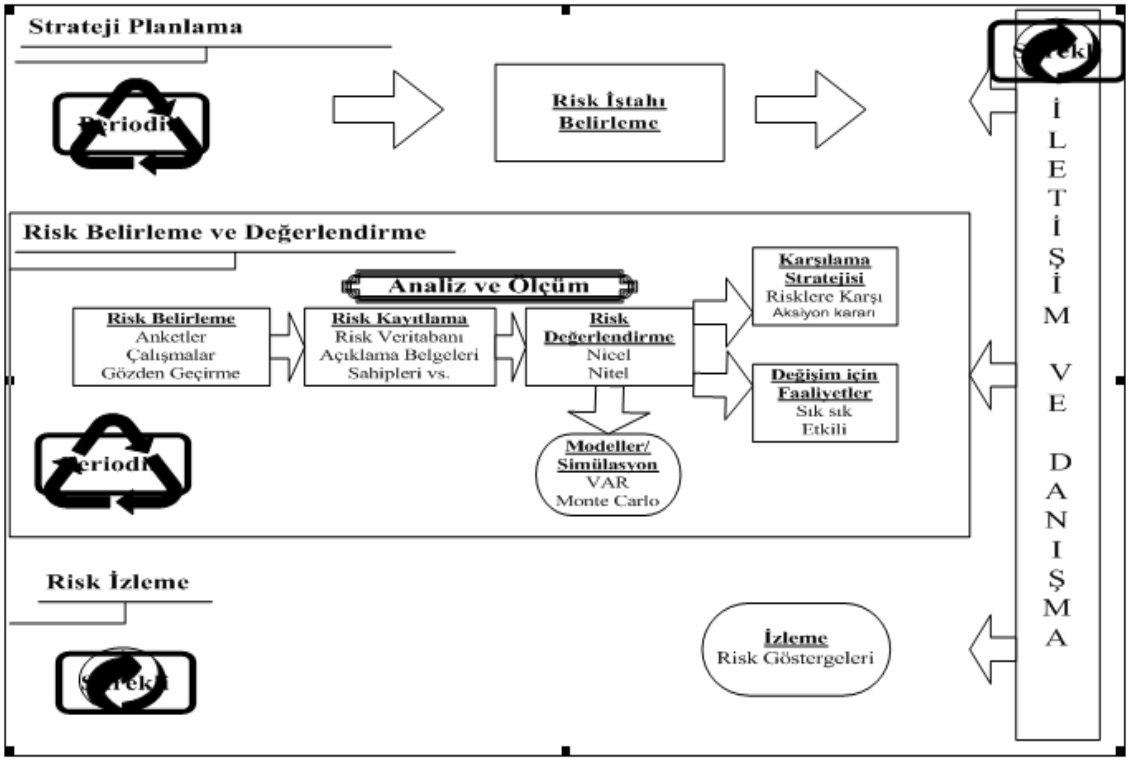
vii) Bilgi & İletişim: Yönetim çalışan sorumluluklarını ve görevlerini ne zaman yerine getirmeleri bilgilerini belirler, ele geçirir ve iletir. Etkin bir iletişim sistemi, kurum içinde yatay ve dikey bilgi ve RY için önemli bir unsur olan raporlamayı da içerir.

viii) Takip: KRY'nin etkin bir şekilde işleyip işlemediğinin belirlenmesi için risk yönetiminin süreçlerinin performans kalitesinin değerlendirilmesi gerekir. İzleme, sürekli izleme faaliyetleri, bağımsız izleme faaliyetleri veya her ikisinin bir kombinasyonu şeklinde yerine getirilir. Sürekli izleme faaliyetleri kurum faaliyetlerinin normal seyrinde meydana gelir. Faaliyetlerin bünyesinde eklemlenmiş olup süreklilik arz eder ve faaliyetle eş zamanlı olarak gerçekleşir. Bağımsız izleme, faaliyet sona erdikten sonra yapıldığından, problemlerin sürekli izleme faaliyetleri aracılığıyla tespit edilmesi daha kolay ve etkindir (COSO,2004; Kayım, 2006).

KRY'nin "etkin" olup olmadığına karar vermek için sözü geçen sekiz unsurun mevcut olduğunu ve etkin bir şekilde işleyip işlemediğini değerlendirmek gerekir. Nitekim bu unsurlar KRY'nin etkinlik kriterleridir.

4.2 Kurumsal Risk Yönetim Süreci

Şekil 4.2 ile en genel haliyle bir risk yönetim süreci gösterlimektedir.



Şekil 4.2 : KRY süreci (Vogel, 2006)den tasarlanmıştır.

4.2.1 Risklerin belirlenmesi ve tanımlanması

İlk olarak risk unsurlarının belirlenmesi sırasında tanımlanan hedeflerin gerçekleştirilmesi üzerinde etkisi olabilecek sebeplerin ve olayların, kapsamlı bir listesinin oluşturulması gerekmektedir. Ne gibi olayların ortaya çıkabileceğinin belirlenmesi sonrasında olaya sebep olabilecek kritik ve temel unsurların ve senaryoların belirlenmesi oldukça önemlidir (TÜSİAD, 2008a).

Olay belirleme işletme stratejisinin gerçekleştirilmesi ve amaçlara ulaşılmasını etkileyebilecek olası olayları ve etkileme sonuçlarını içermektedir. Bu belirlemede riskler, onların içerdiği fırsatlar ve her ikisini içerebilen olası olaylar arasındaki ayrım da yer almaktadır. Yönetim olası olaylar arasındaki ilişkileri belirler ve kurum çapında genel risk dili yaratmak, desteklemek ve olaylara portföy bakış açısıyla yaklaşılmasını sağlamak üzere olayları sınıflandırır (Küçük, 2007).

Riskleri belirlemek için sorulabilecek bazı sorular şu şekilde olabilir;

- Kontrol için en çok çabayı nereye harcarsınız ?
- Hangi alanlar önemli yönetim raporlarına maruz kalıyor?
- Nerede önemli kaynaklarınızı harcamak zorunda kalıyorsunuz?
- Fırsatların avantajlarını alırken anahtar engeller nelerdir?
- Büyümeyi engelleyen nedir?
- Örgüt içinde insanlar nelerden şikayet ediyorlar?
- Eğer siz şirkette bir şeyi düzeltebilseydiniz, bu ne olurdu?

Riskleri belirleme şekillerini ikiye ayırmak gerekir, çünkü kurumda riskler birçok kez belirlenebilir.

Risklerin ilk defa belirlenmesi: Bir kurumda risk yönetimi ilk defa kurgulanırken kurumun karşı karşıya olduğu bütün riskler tespit edilir.

Risklerin sürekli olarak belirlenmesi: Risk yönetim sürecinde mevcut risklerdeki değişiklikler izlenerek risk kütüğünde yer alıp da artık risk olmaktan çıkan riskler ile yeni ortaya çıkan riskler tespit edilir ve buna göre risk kütüğü sürekli olarak güncellenir. Risklerin belirlenmesinde farklı bilgi toplama ve değerlendirme teknikleri kullanmak mümkündür (Derici ve diğerleri, 2007).

Risklerin tanımlanması için kontrol listeleri, kayıtlara ve deneyimlere bağlı çıkarımlar, akış diyagramları, tartışmalar, sistem analizleri, senaryo analizleri ve sistem mühendisliği gibi teknikler kullanılmaktadır. Ayrıntılı liste Çizelge 4.1'de yer almaktadır. Kullanılan yaklaşım, gözden geçirilen aktivitelerin doğasına, risk tiplerine, kurumun iç unsurlarına ve risk yönetim çalışmasının amacına bağlı olarak değişecektir. Kurumdaki tüm olası risklerin belirlenememesi, risk yöneticilerinin bu riskler ile başa çıkmasını engelleyecek ve bu risklerin potansiyel zararlarını ortadan kaldırma ihtimalini de azaltacaktır (TÜSİAD, 2008a).

Çizelge 4.1 : Risk belirleme teknikleri örnekleri (COSO, 2004).

• Şahsi Değerlendirmeler veya diğer uygulama çalışmaları	• İş süreçlerini araştıran, iç ve dış faktörleri tanımlayan ve etkilerini belirleyen çalışmalar
• Görüşmeler ve Mülakatlar	• Endüstri kıyaslamaları
• Anketler	• Senaryo analizi
• Beyin Fırtınası Grupları	• Risk değerlendirme-analiz çalışmaları
• Olay araştırma,	• Denetim ve inceleme
• SWOT analizi	• Tehlike&İşletilebilirlik çalışmaları
• Risk danışmanları	• Değer zinciri analizi
• Süreç haritalama	• İş süreç analizi business
• Kontrol listeleri	• Akış kartları

En yaygın olarak kullanılan yöntemlerden bazıları aşağıda yer almaktadır.

Mülakatlar ve Atölye Çalışmaları: Kurum içinden veya dışından, yönetici ve personelin tecrübe ve bilgi birikiminden faydalanma amacıyla yapılan çalışmalardır. Mülakatlarda, kurumun riskleri konusunda mümkün olduğu kadar fazla görüş ve tecrübeden faydalanmak amaçlanarak işi bilen kilit personel ile görüşülür. Atölye çalışmaları da mümkün olduğu kadar farklı fikirlerin ortaya çıkmasını sağlamak amacıyla, kilit personel ile yapılan tartışmalar ve değerlendirmelerdir.

Odak Grubu (Focus Group) Çalışmaları: 5-9 kişi ile yapılan ve beyin fırtınası şeklindeki fikir yürütme ve tartışmaları içeren çalışmalardır. Bu çalışmalar aynı

zamanda, mülakat ve atölye çalışmalarında elde edilen sonuçların pekiştirilmesi için önemli bir işlev görür.

Olay Envanteri: Benzer kurumlarda gözlemlenen olayların ayrıntılı listesinden oluşur.

Dahili Analiz: Birimlerin personel toplantıları aracılığı ile yaptıkları müzakerelerdir.

Eski Veriler: Geçmişte yaşanmış olayların sebep ve kökenlerinin araştırılmasıdır.

İşlem Akış Analizi: Girdiler, görevler, sorumluluklar ve çıktıların bir süreç olarak ele alınıp incelenmesidir.

Uyarıcı Gösterge: Daha önceden belirlenmiş ve aşılması halinde yönetimi harekete geçirecek, sayısal ya da sayısal olmayan eşik değerlerdir (Derici ve diğerleri, 2007).

4.2.2 Risklerin analiz edilmesi ve ölçülmesi

Belirlenen risklerin nasıl yönetilmeleri gereğinin belirlenmesi için temel oluşturmak üzere riskler değerlendirilir ve analiz edilir. Değerlendirme ve analizinde riskin hem olma ihtimali hem de etkisi dikkate alınmaktadır. Risk değerlendirme ve analiz çalışmaları kapsamında kullanılan çeşitli ve çok sayıda yöntem ve teknik bulunmaktadır (Küçük, 2007). Çalışma kapsamında yapılan araştırmalar sonucunda en yaygın olarak kullanılan ve etkin sonuçlar sağlayan risk değerlendirme ve analiz yöntem ve teknik örnekleri Çizelge 4.2'de verilmiştir.

Çizelge 4.2 : Risk analiz teknikleri örnekleri (COSO,2006).

Risk Analizi Yöntem ve Teknikleri-Örnekler	
• Piyasa araştırması	• Ar-Ge
• İş Etki analizi	• Gözlem
• Bağımlılık modelleme	• GZFT analizi
• Olay ağacı analizi	• İş süreklilik planlama
• Tehlike analizi	• Reel opsiyon modelleme
• Risk&belirsizlik koşullarında karar alma	• İstatistiksel çıkarsamalar
• Merkezi dağılım ve eğilim ölçümleri	• Operasyonel, Politik, Ekonomik, Sosyal, Teknolojik, Teknik, Yasal, Çevresel Analiz
• Hata ağacı analizleri	• Hata Modu &Etki Analizi-HMEA

Risk analizi risklerin sebeplerinin, olumlu/olumsuz etkilerinin ve bu etkilerin ortaya çıkma ihtimallerinin belirlenmesinden oluşur. Risk analizi sırasında bir ön analiz yapılmasında fayda bulunmaktadır. Böylelikle daha detaylı analize geçmeden önce aynı tip riskler bir araya toplanabilir veya düşük önemdeki riskler kapsam dışında değerlendirilebilir. Kapsam dışında olması öngörülen riskler de kayıt altına alınmalı ve gelişimleri izlenmelidir (TÜSİAD, 2008a).

4.2.2.1 Mevcut kontrollerin incelenmesi

Risklerin azaltılması için var olan süreçler, araçlar veya uygulamalar ve bunların zayıf/kuvvetli yönleri incelenmelidir. Mevcut kontroller daha önce yapılmış risk analizleri sonucunda tasarlanmış ve günlük ihtiyaçları yeterli düzeyde karşılamış olabilir. Ancak bu kontrol tasarımlarının şirketin mevcut durumdaki ihtiyaçlarını karşılamada ne derece yeterli olduğu belirlenmelidir (TÜSİAD, 2008a).

4.2.2.2 Etkiler ve ihtimal

Bir olayın birden fazla sonucu olabilir ve değişik iş hedeflerinin gerçekleştirilmesini etkileyebilir. Tek başına etki veya ihtimal riskin öneminin belirlenmesinde kullanılmamalıdır. Risklerin önem seviyesi, etkiler ve ihtimallerin bir araya gelmesi ile oluşturulmalıdır Etki ve ihtimalin tahmin edilmesinde istatistiksel analiz ve hesaplamalar kullanılabilir. (TÜSİAD, 2008a)

Analiz sırasında belirlenmesi gereken en önemli bulgulardan biri olayın ortaya çıkma olasılığıdır. *Olayın ortaya çıkma olasılığı*nı belirli bir zaman dilimi içinde operasyonel kayıp türlerinin ortaya çıkma olasılığının tahmini olarak tarif edilebilir.

Belirli bir olayın ortaya çıkma olasılığının hesaplanması şöyle ifade edilir;

$$\text{Olayın ortaya çıkma olasılığı} = \frac{\text{Olayın, belirli bir zaman içinde yaşanan tekrar sayısı}}{\text{Toplam işlem sayısı}},$$

Belirli bir olayın gelecekte ortaya çıkma olasılığı geçmişte yaşanmış tekrarlarla benzerdir. Ancak değişen ürün ve hizmetler ile piyasa koşulları ve teknolojide yaşanan hızlı değişimler göz önünde bulundurulduğunda, yukarda belirtilen yöntemin sadece sık yaşanan olayların tahmini için daha geçerli olacağı sonucuna varılabilir.

Ortaya çıkma sıklığı düşük olan olaylar için senaryo analizi yapılması daha uygundur.

Senaryo Analizi"nde ise beklenmedik olaylarla ilgili geliştirilen her senaryo için ortaya çıkma olasılığı ve etki değerleri varsayılarak operasyonel risklerin olası büyüklükleri belirlenmeye çalışılmaktadır. Subjektif nitelik taşıyan senaryo analizi, daha çok belirsiz ve şüpheli durumlarda kullanıma uygundur.

Olayın ortaya çıkma olasılığı ile birlikte hesaplanması gereken diğer olgu ise *olayın etkisi*'dir. Olayın işletme hedef ve stratejilerini ne derecede etkilediği sorularak istenen sonuçlara ulaşılabilir.

Son olarak olasılık ve etki sonuçları kullanılarak *olayın önem derecesi* hesaplanır. Olayın önem derecesi riskin önemini ve ne kadar kritik olup olmadığını gösteren bir sonuçtur. Operasyonel kayıp olayının önem derecesi, meydana gelen olayın riskini ölçmede kullanılan en basit yöntemdir.

Olayın önem derecesi = [Olayın ortaya çıkma olasılığı(%)] x [Olayın etkisi(TL,$,€)]

Bu tip analizlerde bireylerin tahminleri ve grupların tahminleri arasında bir denge sağlanmalı ve analiz sonucunda ortaya çıkabilecek farklı tahminler arasında bir görüş birliğine varılması sağlanmalıdır. Analizler her ne kadar sübjektif olsa da mutlaka bazı kritik risk göstergeleri ile ilişkilendirilmelidir. Etkiler ve ihtimaller analiz edilirken amaca en uygun bilgi kaynakları ve teknikler kullanılmalıdır. Bilgi kaynaklarına örnekler Çizelge 4.3'de verilmektedir.

Çizelge 4.3 : Bilgi kaynakları.

Mevcut eski kayıtlar	Pazar araştırmaları	İlgili basılmış kaynaklar
Oylama sonuçları	Deneyler ve prototipler	Uzman görüşleri
Deneyler	Yapılan inceleme sonuçları	Uygulamalar ve tecrübeler
Farklı kaynaklardan alınmış istatistiksel veriler	Ekonomik, teknik veya diğer modeller	

Analizler sırasında kullanılan varsayımlar mutlaka belgelenerek kayıt altına alınmalıdır. Örnek kayıt formu Şekil 4.3'deki gibi olabilir.

RİSK KAYIT FORMU

Risk inceleme tarihi ----------

kayıt yapan:----------Tarih ----------

Fonksiyon/aktivite----------

İnceleyen :----------Tarih ----------

Ref	Risk : Ne olabilir ve Nasıl olabilir	Olay meydana geldiğinde sonuçları		Mevcut kontrollerin yeterliliği	Sonuçların sıralanması ve derecelendirilmesi	Olma ihtimalinin derecelendirilmesi	Risk Seviyesi	Risk Önceliği
		Sonuçlar	Olma ihtimali					

Şekil 4.3 : Risk kayıt formu örnegi (Tesla, 2006).

Risk kayıt formunda genel olarak riskin ne ve neden olabileceği, risk meydana gelirse bunun sonuçları ve riskin olasılığı, ilgili riske yönelik uygulanan mevcut kontrol faaliyetlerinin yeterliliğinin değerlendirilmesi, riskin meydana gelmesi halinde sonuçlarının sıralanması ve derecelendirilmesi, riskin olasılığının derecelendirilmesi, riskin işletmeyi etkileme şiddeti açısından seviyesi ve tüm bu değerlendirmelerden sonra bu riskin işletme tarafından yönetilmesi gerekliliğini ve önemini belirten riskin önceliği kapsamında hazırlanmış bölümler bulunmaktadır. Formdaki bu bölümler doldurularak yapılan çalışmaların kayıt altına alınması ve KRY için önemli olan doğru ve zamanlı bilginin elde edilmesi açısından önem taşımaktadır (Küçük, 2007).

4.2.2.3 Analiz tipleri

Risk analizi; analiz edilecek riske, analizin amacına, erişilebilen bilgi ve kaynakların seviyesine bağlı olarak farklılık gösterecektir. Analiz duruma göre kalitatif (niteleyici), yarı-kantitatif (yarı-niceleyici), kantitatif (niceleyici) veya bunların bir birleşimi sonucunda karma bir analiz olabilir. Bu analiz tiplerini karmaşıklık ve maliyet

özelliklerine göre en yüksekten düşüğe sırasıyla kantitatif, yarı-kantitatif ve kalitatif şekilde sırlamak mümkündür (TÜSİAD, 2008a). Bu üçlünün teker teker yada kombinasyon olarak kullanımı, mevcut verilere ve aranan doğruluk derecesine bağlıdır. Pratikte, kalitatif analizler genelde risk seviyesinin belirlenmesinde kullanılır. Daha spesifik ve kesin belirlemelere ihtiyaç duyulduğunda kantitatif analizler uygulanır (Riskactive, 2008).

(a) Kalitatif (Niteleyici) Analiz

Kalitatif analiz, olayların potansiyel etkilerinin derecesini ve bunların ortaya çıkma ihtimallerini, kelimelerden oluşan skalalar üzerinden analizi gerçekleştirenlerin bireysel yargıları ile ortaya çıkan sonuçlar ile ifade etmektedir. Bu skalalar ihtiyaca göre düzenlenebilir ve değişik riskler için değişik tanımlamalar kullanılabilir (TÜSİAD, 2008a). Farklı durumlardaki farklı riskleri, uygunluğu sağlamak için çeşitlendirmek, benimsemek ve düzeltmek için kullanılır.

Kalitatif analiz aşağıdaki durumlarda kullanılabilir (Riskactive, 2008):

- Risk seviyesi, ayrıntılı bir analizde harcanan zaman ve çabayı karşılamadığında,
- Daha detaylı analiz gerektiren riskleri belirleme için yapılan hazırlık çalışmalarında,
- Kararlar için bu tip analizlerin uygun ve yeterli olduğu durumlarda,
- Kantitatif analiz için gerekli veri veya kaynaklar yetersiz olduğunda,
- Söz konusu riskin yapısal özellikleri gerekli kıldığında,
- Risklerin ölçüme olanak tanımadığı zamanlar,
- Verilerin elde edilmesinin ve analizinin maliyet açısından elverişli olmadığında.

Kalitatif analiz mümkün olduğunca geçmişte yaşanan olaylara dayandırılmalı ve bu olaylar ile ilgili veriler ile beslenmelidir.

(b) Yarı-Kantitatif (Yarı-Niceleyen) Analiz

Yarı-kantitatif analizde kalitatif analizde kullanılan skalalardaki kelimelerden oluşan tanımlamaların yerini rakamlar almaktadır. Bu yöntemde daha geniş derecelendirme skalaların uygulanmasını sağlamak amaçlanmıştır. Ancak bu yöntemde de

derecelendirme, analizi gerçekleştirenlerin bireysel yargıları ile belirlenmektedir. Bu nedenle riskler için skala üzerinde gerçekleştirilen derecelendirme etki ve ihtimal tahminlerinin ölçülmüş değerlerini içermemektedir Yarı-kantitatif analiz etkileri ve olasılıkları çok yüksek olan risklerin aralarındaki farkların ortaya konmasında da eksik kalabilecektir (TÜSİAD, 2008a).

Her kalitatif ölçek için seçilmiş sayı, olasılık ya da sonucun asıl boyutu için gerçek bir ilişkiyi doğrulamayabilir. Sadece analitik amaçlar için büyüklük sıralaması sağlar. Kalitatif analizlerle elde edilenden fazla olarak, risklerin daha detaylı biçimde önceliklendirilmesini sağlar. Kantitatif analizlerde olduğu gibi gerçek değerleri sağlamaz (Riskactive, 2008).

(c) Niceleyen (Kantitatif) Analiz

Kantitatif analizde, değişik kaynaklardan alınan veriler kullanılır. Bu tip analizlerin kalitesi, sayısal verilerin doğruluğuna, bütünlüğü ve kullanılan modelin geçerliliğine dayanır. Olasılık genelde ihtimal, maruz kalma ya da ihtimal ve maruz kalmanın kombinasyonu olarak açıklanır. Örneğin, inceleme sonucunda bir işletmede 50 kapıdan 20'sinin hatalı şekilde kapandığı ve bunun küçük yaralanmalara sebep olduğu saptanmış. Demek ki burada %40 oranında yaralanmaya maruz kalma söz konusudur. Yaralanma ihtimali, kişinin hatalı kapı kullanma ve elini kapıya sıkıştırma olasılığına bağlıdır. Bu bilgi, geçmiş istatistiklerden elde edilebilir. Sonuç kayıp, zarar görme, dezavantaj ya da kazanç gibi bir çıktı olabilir. Bu ölçülebilir ya da ifade edilebilir. Eğer birkaç yıllık veri varsa, daha doğru bir çalışma yapılabilir. Kurumlar, mümkün olduğunca geniş bir veri bankası oluşturmalıdır (Riskactive, 2008).

Potansiyel etkiler belirli bir olayın veya olaylar dizisinin sonuçlarının modellenmesi ile bulunabileceği gibi geçmiş çalışmalardan veya olaylardan da istatistiksel olarak çıkartılabilir. Etki; parasal, teknik, insana gelebilecek zarar veya diğer bir zarar kriteri cinsinden ortaya çıkartılabilir. Bazı durumlarda aynı olayın risk derecesinin belirlenmesi için birden fazla rakamsal değer kullanılması gerekebilir. Etkilerin ve ihtimallerin belirsizlik ve değişkenliği analiz esnasında göz önünde bulundurulmalı ve etkin bir şekilde raporlanmalıdır (TÜSİAD, 2008a).

Kantitatif teknikleri genellikle, belirli aralık ya da oranlar kullanılarak riskin olasılığını yada etkisini hesaplamak için yeterli bilginin bulunmaması ve aşırı karmaşık ve özel faaliyetler için artan hassas incelemeler gerektiğinde kalitatitif tekniklerin desteklenmesi gerektiğinde kullanılır. Çizelge 4.4'de analiz tiplerine ilişkin örnekler yer almaktadır.

Çizelge 4.4 : Analiz tipleri (Riskactive, 2008).

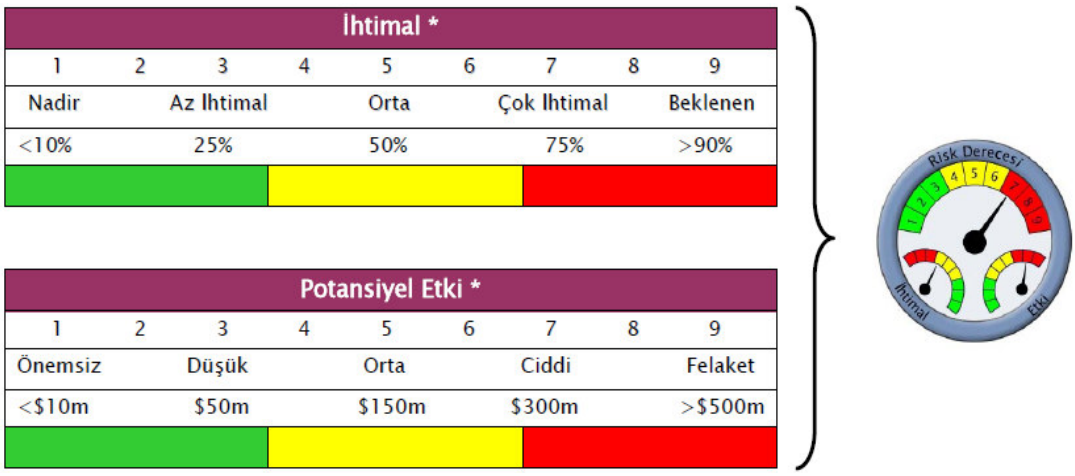
Yaklaşımlar	**Kalitatif**	**Kantitatif**
	Anahtar performans göstergesi	Maliyet/Kar odaklı yaklaşım
Yukardan	Anahtar kontrol göstergesi	Tesadüfi dağılımlar
Aşağı	Anahtar risk göstergesi	Uç değer teorisi
	Fayda değer analizi	
	Karar ağacı analizi	Güvenilirlik teorisi yaklaşımı
Aşağıdan	Senaryo analizi (subjektif)	Simülasyon modeli
Yukarı	Süreç riski analizi	Senaryo analizi
	Uzmana danışma/görüşme	

4.2.2.4 Duyarlılık analizi

Risk analizi kapsamında yapılan varsayımlar kesin ve kusursuz olamayacağından belirsizliğin varsayımlar ve kullanılan veri üzerindeki etkilerinin belirlenmesi için duyarlılık analizi yapılması gereklidir. Duyarlılık analizi aynı zamanda potansiyel kontrollerin ve KRY aksiyonlarının uygunluğunun ve etkinliğinin test edilmesi için de kullanılabilecek bir analiz tipidir. Temel olarak belirli senaryolar altında modelin esnekliğinin belirlenmesi için kullanılır.

4.2.3 Risklerin değerlendirilmesi ve önceliklendirilmesi

Risklerin değerlendirilmesi, muhtemel risklerin gerçekleşme ihtimalini, gerçekleşmesi halinde olası etkilerinin önceden tahmin ve tespit edilmesini ve yönetimin bu riskleri göze alma düzeyinin belirlenmesini içeren süreçtir. Riskleri önceliklendirmek, zaman olarak gerçekleşme aralığı ve kurumun başarısına etkisi açısından risklerin sıralanmasını ifade eder. Etki ve ihtimal düzeyleri, risklerin önemlilik düzeylerinin göstergesidir. Bu yöntemde, Şekil 4.4'de görüldüğü gibi önce ihtimal ve etkiler bulunur ve sonucunda risk derecesi belirlenerek riske karşı önlem almaya geçilir.



Şekil 4.4 : Risk değerlendirme skalaları (Saka, 2006).

Risklerin gerçekleşme ihtimali değerlendirilirken; beklenen (yüksek), orta ve nadir (düşük) olmak üzere üç düzeyli bir tablonun kullanılması en sık görülen değerlendirme seçimlerindendir. Bu üç düzeyi açıklamak gerekecektir;

Yüksek (3): Bir yıllık zaman dilimi içinde gerçekleşme olasılığının bulunmasıdır.

Göstergeler: * Gelecek on yıl içinde bir çok defa gerçekleşme potansiyeli

* Son iki yıl içinde gerçekleşmiş olması

* Dış etkenler nedeniyle kontrolün çok güç olması

Orta (2): On yıllık zaman dilimi içinde gerçekleşme olasılığının bulunmasıdır.

Göstergeler: * Gelecek on yıl içinde birden fazla gerçekleşme potansiyeli

* Dış etkenler nedeniyle kontrol güçlüğü çekilmesi

* Faaliyetle ilgili geçmiş deneyimler

Düşük (1): On yıllık zaman dilimi içinde gerçekleşme olasılığının bulunmamasıdır.

Göstergeler : * Şu ana kadar hiç gerçekleşmemiş olması

* Gerçekleşmesi halinde büyük şaşkınlık yaratacak olması.

Risklerin etki düzeyleri değerlendirilirken de yine üç kademeli değerlendirme aracı kullanılması en yaygın uygulamalardandır. Bu üç kademe ise;

Yüksek (3) :* Kamuoyunun son derece duyarlı olması

* Kurumun temel hedefleri üzerinde hayati etkilerinin söz konusu olması

* Mali sonuçlarının çok büyük boyutta olması

Orta (2) : * Kamuoyunun önemli derecede duyarlılık göstermesi

* Kurumun temel hedefleri üzerinde önemli etkilerinin olması

* Mali sonuçlarının kaygı verici boyutta olması

Düşük (1) : * Kurumun temel hedefleri üzerinde düşük derecede etkili olması

* Kamuoyu duyarlığının düşük düzeyde olması

* Mali sonuçlarının tolere edilebilir olması gibi durumları ifade etmektedir.

Şekil 4.5'de verilmiş matris risk değerlendirme sürecinin sonuçlarını özetlemektedir. Her iş döngüsü/süreci, iş stratejisine olan önemine ve kontrol/süreç konuları olasılığına dayalı olarak risk değerlendirme katılımcıları tarafından değerlendirilmiştir.

R= O X Ş

	SONUÇ				
OLASILIK	ÇOK CİDDİ 5	CİDDİ 4	ORTA 3	HAFİF 2	ÇOK HAFİF 1
ÇOK YÜKSEK 5	YÜKSEK 25	YÜKSEK 20	YÜKSEK 15	ORTA 10	DÜŞÜK 5
YÜKSEK 4	YÜKSEK 20	YÜKSEK 16	ORTA 12	ORTA 8	DÜŞÜK 4
ORTA 3	ORTA 15	ORTA 12	ORTA 9	DÜŞÜK 6	DÜŞÜK 3
KÜÇÜK 2	ORTA 10	ORTA 8	DÜŞÜK 6	DÜŞÜK 4	DÜŞÜK 2
ÇOK KÜÇÜK 1	DÜŞÜK 5	DÜŞÜK 4	DÜŞÜK 3	DÜŞÜK 2	DÜŞÜK 1

Şekil 4.5 : Risk derecelendirme/sınıflandırma matrisi (Andaç, 2008).

Bu tür uygulamalarda, her riskin matris üzerindeki etki ve ihtimali yukarıda belirtilen hususlar ışığında, sayısal olarak 1 ile 5 arasında tespit edilir. Bu yöntemde, riskler matris üzerinde bulundukları noktalara göre (1x1=) 1'den (5x5=) 25'e kadar puanlandırılır ve sıralanır. Matris üzerinde, ihtimal ve etki düzeylerinin bileşiminden oluşan noktalar şu anlamları ifade eder:

*** Yüksek:** Önemlilik düzeyi 15-25 arasında olan riskler grafikte kırmızı alanda yer alır. Bunun anlamı, bu risklerin kurum için çok önemli olduğu ve bunlara karşı önlem alınmasının çok gerekli olduğudur. Bu durum aynı zamanda, konunun en üst yöneticinin mutlaka ilgilenmesi ve politika belirlemesi gereken bir ciddiyete sahip olduğunu gösterir. Risk düzeyinin yüksek olması, artık risk seviyesinin göze alınabilen risk seviyesinden oldukça yüksek olduğu anlamına gelir.

*** Orta**: Önemlilik düzeyi 8-15 arasında olan riskler grafikte sarı alanda yer alır. Orta düzey, artık risk seviyesinin göze alınabilen risk seviyesinden biraz yüksek olduğu durumdur.

*** Düşük**: Önemlilik düzeyi 1-6 arasında olan riskler grafikte yeşil alanda yer alır.

Risklerin önemlilik düzeyleri, kurumun risk kütüğünde, 'düşük', 'orta', 'yüksek' veya rakamsal olarak, 1, 2, 3, 4, 5 şeklinde gösterilir (Derici ve diğerleri, 2007).

Ayrıca aşağıdaki Çizelge 4.5'deki ve Çizelge 4.6'daki tanımlanmış skalaları kullanılarak da anahtar riskler "önem" ve "olasılık" sırasına göre sıralanabilir.

Çizelge 4.5 : Risklerin önem şiddetine göre derecelendirme ve tanımlama tablosu (www.knowledge.com).

Seviye	Açıklayıcı	İşe Etkinin Tanımlaması
7,8,9	Büyük	Çok önemli finansal kayıp ihtimalini gösterir ve kurumun büyük değişiklikleri olmadan devam edebilme kabiliyetini tehlikeye sokabilirler. Denetim bağlantısı gerektirebilir.
4,5,6	Orta	Finansal kayıp orta seviyededir, önemli olabilir, ve genel bilgilendirme gerektirebilir. Yönetim konuyla ilgilidir zamanlı uygun bir biçimde yetkinleştirmeye odaklanır.
1,2,3	Önemsiz	Küçük finansal kayıplar olabilir. Yönetimin dikkatini gerektirmez. Riskin oluşmasını karşılarken muhtemelen proses değişiklikleri gerektirmez.

Çizelge 4.6 : Risklerin olasılık şiddetlerine göre derecelendirme ve tanımlama tablosu (www.knowledge.com).

Seviye	Açıklayıcı	İşe Etkinin Tanımlaması
7,8,9	Olası	Birçok durumda olması beklenen gelecek olay veya olaylar.
4,5,6	Makul	Gelecekdeki olay veya olayların olasılığının çok uzakdan fazla olasıdan az olması.
1,2,3	Az ihtimal	Gelecek olay veya olayların yanlızca istisnai durumlarda olması.

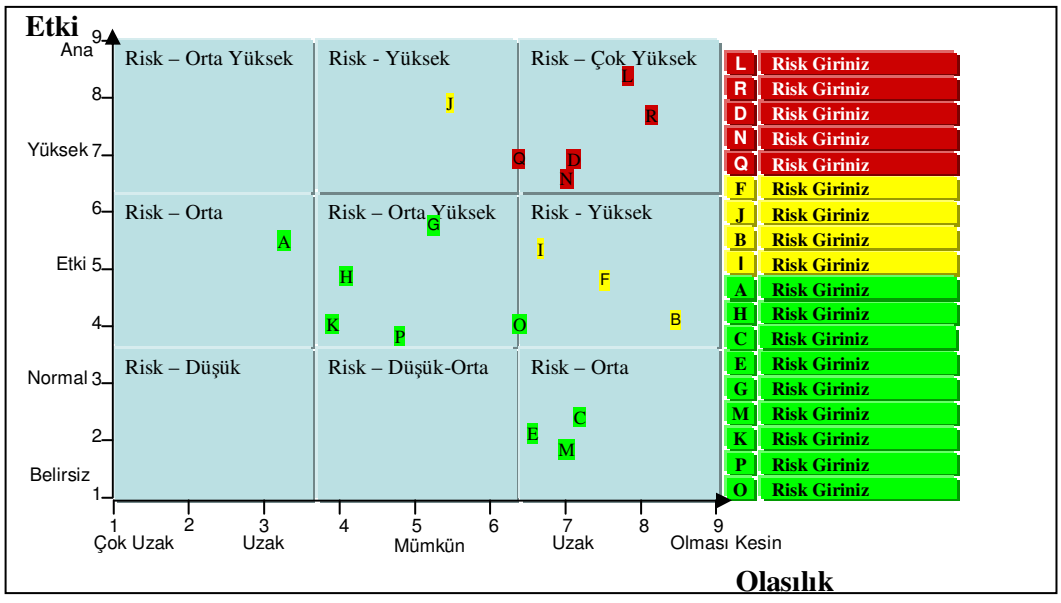
Risklerin bu şekilde değerlenmesi sürecinde kurumun hedefleri ve alternatif fırsatların potansiyel sonuçları göz önüne alınmalıdır. Hedefler ile uyumlu olan birden fazla alternatif olması durumunda, seçim yapılırken alternatiflerin potansiyel kayıpları ve kazançları objektif bir şekilde değerlenmelidir. Alternatiflerin arasında yapılacak seçim ise şirketin risk alma isteği seviyesine uygun bir şekilde yapılmalıdır.

Düşük risk grubundaki riskler, rutin prosedürlerle yönetilir. Orta risk grubunda yönetim sorumluluğu özelleştirilmelidir ve yüksek grubundaki riskler ise, üst yönetimin dikkatini gerektiren ve acil müdahaleye ihtiyaç duyan risklerdir.

Riskin önemlilik düzeyinin düşük olması; artık risk ile göze alınabilen risk seviyesinin aynı veya yakın olduğu anlamına gelir. Riskleri önceliklendirme konusunda değişik usuller ve matematiksel yöntemler kullanılabilir. Ancak şunu kabul etmek gerekir ki işin konusu ne kadar rakamlara veya somut verilere dayanırsa dayansın, riskleri değerlendirme/önceliklendirme işi esas olarak yargılara dayanır. Şekil 4.6'da risklerin önceliklendirmesinde oluşma sıklıkları ve yapacakları etkinin büyüklüğü açısından değerlendirme metodu anlatılmaktadır.

Şekil 4.6 : Karşılaşılan riskleri önem ve olasılık faktörüne göre gruplandırma grafiği.

Oluşturulan matrisler risk haritalarına dönüştürülebilir. Kurumsal risk yönetiminin gerekliliği olarak rapor edilmelidir. Aşağıda Şekil 4.7'de çok genel bir haritası taslağı bulunmaktadır

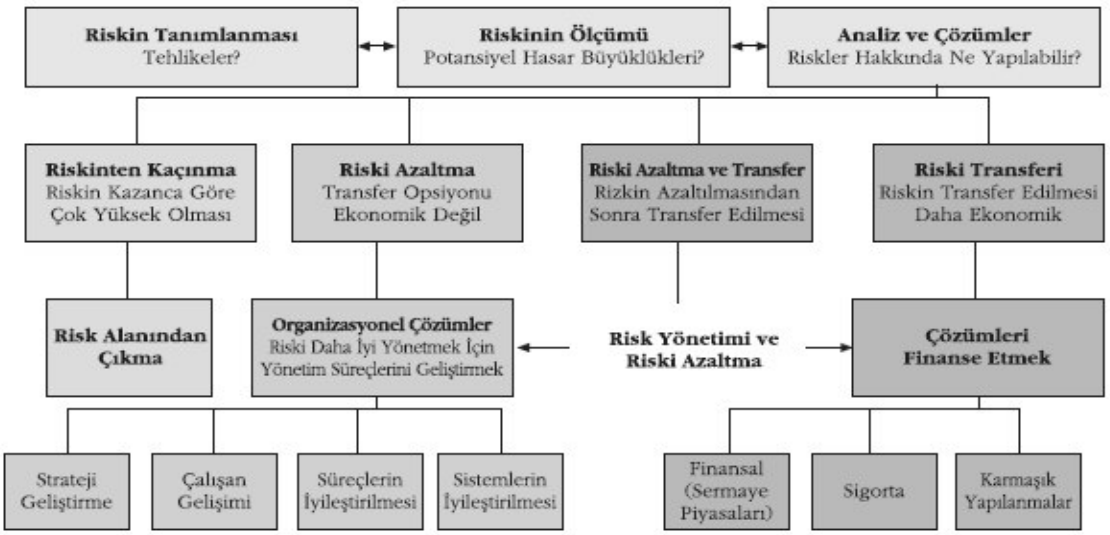


Şekil 4.7 : Örnek risk haritası.

4.2.4 Risklere uygun çözümlerin belirlenmesi ve uygulanmaları

Riskler belirlendikten ve ölçüldükten sonra risk yöneticisi en uygun araçların kombinasyonu ile problemin çözümü için karar almalıdır. Bu adım, risk yönetim aksiyonları için alternatiflerin belirlenmesini, alternatiflerden en uygun olanına karar

verilmesini, uygulama planlarının hazırlanmasını ve uygulanmasını, özetle risk yönetim stratejilerinin belirlenmesini içermektedir. Bu stratejiler Şekil 4.8'de gösterilmektedir.



Şekil 4.8 : Risklere uygun çözüm ve uygulamalar (TÜSİAD, 2008a).

Riskten Kaçınma: Riskin ortaya çıkmasına veya artmasına sebep olan faaliyetlere başlanılmaması veya son verilmesi şeklinde riskten kaçınmak mümkündür. Riskten kaçınma kararı, şirketin risk iştahı yüksek ise uygun olmayabilir. Riskten kaçınma diğer risklerin öneminin artmasına ve/veya fırsatların kaybedilmesine neden olabilmektedir.

Riskin İhtimalinin Azaltılması*:* Uygun kontroller yardımı ile olayların olumsuz etkilerinin ortaya çıkma ihtimalinin azaltılmasıdır.

Riskin Etkilerinin Azaltılması: Olayların olumsuz etkilerinin büyüklüğünün azaltılarak potansiyel kayıpların azaltılması için gerekli kontrollerin belirlenmesi ve uygulanmasını gerektirir.

Riskin Transfer Edilmesi ve Paylaşılması: Riskin bir parçası veya tümünün diğer bir taraf veya taraflarca üstlenilmesidir. Ancak riskin paylaşılması/transfer edilmesi ile riski üstlenen tarafın riski uygun ve etkin bir şekilde yönetememesi riski doğmaktadır.

Riskin Kabul Edilmesi: Risklerin azaltılmasından veya paylaşılmasından sonra geriye bir miktar risk kalacaktır. Bu geriye kalan risk eğer belirlenmez ve uygun şekilde yönetilmez ise şirkete zarar olarak yansıması söz konusu olabilir. Bu risk şirketin risk kriterleri ile karşılaştırılıp hakkında bir aksiyon alınıp alınmamasına karar verilmelidir.

4.2.5 Sürecin sürekli izlenmesi ve gözden geçirilmesi

Etkin bir risk yönetimi sürecinde, risklerin net olarak tanımlanması, değerlendirilmesi ve uygun kontrol ve aksiyonların uygulanması için bir raporlama ve gözden geçirme yapısına ihtiyaç duyulur. Organizasyondaki değişiklikler ve faaliyette bulunulan ortam belirlenmeli ve sistemde uygun değişiklikler yapılmalıdır. İzleme süreci, organizasyonun faaliyetlerine uygun kontrollerin kullanılmasını ve prosedürlerin anlaşılmış ve takip ediliyor olmasını sağlamalıdır. İzleme ve gözden geçirme süreçleri aynı zamanda; uygulanan kontrollerin istenilen sonuçlara ulaşıp ulaşmayacağı, değerlendirmeyi yapabilmek için uygulanan prosedürlerin ve toplanan bilginin uygun olup olmadığı, ve daha kapsamlı bilginin daha iyi kararlar almaya yardımcı olup olmayacağı konularına açıklık getirir. Bu amaçla sayısal ve sayısal olmayan performans ölçüm teknikleri belirlenerek uygulamaların performansı sürekli olarak yakından izlenmelidir. Bu kapsamda sonuçlar da riske göre ayarlanmış (Risk Adjusted) yöntemlerle değerlendirilmeli ve böylelikle risk yönetim uygulamalarının sonuçlarının, işletme sonuçlarına ne derece yansıdığı belirlenmelidir (TÜSİAD, 2008a).

4.2.6 İletişim ve danışma

İletişim ve danışma risk yönetim sürecinin her adımında oldukça önemli bir yere sahiptir. Karar alıcılardan menfaat sahiplerine yapılacak tek yönlü bilgilendirme yerine karşılıklı bir diyalog kurulmalıdır. Karşılıklı görüş alışverişine dayalı bir takım yaklaşımı, risklerin etkin bir şekilde belirlenmesinde, risklerin analiz edilmesi sırasında farklı tecrübelerin bir araya getirilmesinde, risklerin ölçülmesi sırasında değişik görüşlere yer verilmesinde ve risk yönetim stratejilerinin uygulanmasında değişim yönetiminin uygulanmasına yardımcı olacaktır (IRM ve diğ., 2002). Bu yaklaşım yöneticilerin riskleri ve risk yönetim süreçlerini daha iyi anlamalarını, sahiplenmelerini ve desteklemelerini sağlayacaktır. İletişim ve danışma faaliyetlerinin kayıt altına alınması faaliyetlerin hassasiyeti ve büyüklüğü gibi faktörlere bağlıdır (TÜSİAD, 2008a).

4.3 Kurumsal Risk Yönetimi Uygulamada Olgunluk Seviyeleri

Günümüzde kurumsal risk yönetimi işletmelerde temel uygulama, genele uygulama, bugünün en iyi uygulamaları ve yarının en iyi uygulamaları olmak üzere toplam dört

olgunluk seviyesinde uygulanmaktadır. Olgunluk seviyesi, işletmenin kendi KRY içyapısını tanıması açısından önemlidir.

Birinci olgunluk seviyesi, temel uygulamaları kapsamaktadır. Bu seviyede risk yönetimi sadece maddi kayıpların önlenmesine odaklanmaktadır. Bu çerçevede organizasyonlar mevzuata ve yasalara uygunluk açısından risk değerlendirmeleri ve kalitatif risk analizi çalışmaları yapmaktadırlar. Merkezi bir risk yönetim birimi bulunmamakta ve riskler birim bazına inilmeden genel kapsamda belirlenmektedir.

KRY ikinci olgunluk seviyesi, genel uygulamaları kapsamaktadır. Bu seviyede risk yönetimi faaliyetleri kurum içinde birim bazında ve birime özel alanlarda gerçekleştirilir. Bu sayede kurum içinde risk yönetimi anlaşılırlığı sağlanmaya başlanmış ve olay bazlı bilgi akışı elde edilmiştir. Ayrıca bu seviyede kalitatif risk analizleri periyodik olarak gerçekleştirilir.

Üçüncü olgunluk seviyesinde bulunan organizasyonlar, KRY uygulamalarında bugünün en iyi uygulamalarını gerçekleştirmektedirler. Yönetim kadrosunda risk yönetimi sahiplenilmiş ve KRY'ye kurum genelinde yaklaşım sağlanılmıştır. Bu seviyede risk yönetim süreçleri belirlenen iş süreçlerine entegre edilmiş ve risk ile ilgili bilgi ve iletişim temelleri oluşturulmuştur. Bir önceki olgunluk seviyesinde gerçekleştirilmeye başlanılan periyodik kalitatif risk analizleri modellenerek, hissedarlara değer yaratan temel unsurlarla bağlantısı kurulmuştur.

Dördüncü ve en üst olgunluk seviyesi ise gelecekteki en iyi uygulamalardır. Bu olgunluk seviyesi, dünya çapında sınırlı organizasyonlarca uygulanabilmekte olan karmaşık risk yönetimini kapsamaktadır. Bu seviyede risk trendlerinin ve etkilerinin tahmin edilmesine olanak sağlayan risk analiz modelleri gerçekleştirilir. Tüm risk yönetimi, organizasyonun tamamındaki süreçlere entegre edilmiş ve organizasyonun sermaye ve kaynak dağılımları da risk, büyüme ve getirilere odaklanmıştır.

Şirketin boyutu ve içinde bulunulan sektör dinamikleri, Seviye 1'den fazlasını gerektirmeyebilir. şirketlerin bu farkındalığı kritik bir noktada karşımıza çıkmaktadır. şirketler büyüdükçe, içindeki bulundukları ortam daha karmaşıklaştıkça riski etkin yönetmek daha önemli hale gelmektedir (PWC, 2006).

5. KURUMSAL RİSK YÖNETİMİNDE YASAL DÜZENLEMELER

5.1 Kurumsal Risk Yönetiminde Yasal Mevzuatlar

Bugüne kadar denetim, iç denetim, iç kontrol, COSO çerçevesi, düzenleyici otoriteler, skandallar ve Sarbanes Oxley yasası gibi konu başlıklarında birçok makale yazılmış ve araştırma yapılmıştır. Risk faktörlerinin azaltılması, etkinliğin artırılması ve verimli operasyonları elde etme amaçları artık şirketlerin giriş lobisindeki duvarlara asılı duran şirket misyonu tabelalarında yer almaktadır.

Risk yönetimi ve iç denetimde uluslararası standartlar bir kuruluşun kendi sektörüne, süreçlerine ve standartlara göre bir risk çerçevesi oluşturmasına yardımcı olmaktadır. Bu standartlar, bir kuruluşun hem kendi sektörünün özelliklerini, hem de kendi iş süreçlerini/verilerini dikkate alarak, bunları uluslararası standartlarla birleştirmesinde ve bir risk çerçevesi oluşturmasında bir adım olmaktadır (Meriç, 2004).

Bu standartlar içinde en çok kabul görmüş ve en yaygın uygulanan yasal düzenlemeler bu bölümde açıklanmıştır.

5.1.1 Sox - Sarbanes-Oxley Act

Sarbanes Oxley Kanunu, ABD'de Sermaye Piyasası Kurumunun dengi olan Securities and Exchange Comission (SEC) tarafından, ABD sermaye piyasalarında faaliyet gösteren yerli ve yabancı firmalar için getirilmiş en önemli düzenlemedir. 30 Temmuz 2002 de Başkan George W. Bush "Sarbanes-Oxley Act of 2002" yi imzalamıştır. Firmaların özellikle kurumsal yönetim kadrolarına ve denetim komitelerine ciddi yükümlülükler ve yeni raporlama şartları getirmiştir (Karaca, 2007).

Sarbanes Oxley yasasının dünyada yarattığı iç kontrol çılgınlığı, dalga dalga tüm ülkelere yayılmış ve bazen aynı, bazense farklı başlıklarla çıkmıştır.

SEC'e bağlı ABD şirketleri 15 kasım 2004 itibari ile ve SEC'e tabi uluslararası şirketler de 15 Temmuz 2005 tarihi itibariyle bu kanunu yönetim mekanizmalarına entegre

etmek zorundadır. Bu bakımdan Türkiye'de SEC'e tabi uluslararası firmaları da yakından ilgilendiren bir konu olması nedeniyle Sarbanes Oxley 'in incelenmesi yararlı olacaktır. Türkiye de Enron, Xerox ve Worldcom vakalarını yaşamamak için Sarbanes Oxley Kanununun hükümlerini SPK'nın Seri: X No:19 Tebliği ile Türkiye'de uygulamaya geçirmiştir (Gökalp, 2005).

Bu kanun;

- Kurumsal iletişim (yöneticilerin sorumluluklarını da içerecek şekilde),
- Denetim firmalarının düzenlenmesi,
- Kurumsal raporlama , konularında değişiklikler getirmiştir.

Sarbanes Oxley Kanunu; muhasebe gözlem kurulunun kuruluşu ve işleyişi, denetim firmasının bağımsızlığı, şirketin sorumluluğu, mali bilgilerin arttırılması, analiz çıkar çatışmaları, komisyon kaynakları ve otoritesi, çalışmalar ve raporlar, kurumsal ve suç unsuru taşıyan suiistimal sorumluluğu, beyaz yakalılar suçları ile ilgili cezaların arttırılması, kurumsal vergi iadeleri ve kurumsal suiistimal ve sorumluluk konuları olmak üzere 11 ana başlıktan oluşmaktadır (SOX, 2002).

Yasanın 302 ve 404 numaralı maddeleri çerçevesinde şirketlerin finansal raporlamaları üzerindeki risklerin belirlenmesi, belirlenen risklere ilişkin kontrollerin dokümante edilmesi ve değerlendirilmesi zorunlu tutulmuş, kontrollerin etkinliğinden şirket yöneticileri direk olarak sorumlu tutulmuştur. Yasa ile birlikte gelen ağır cezai yaptırımlar şirket yöneticileri başta olmak üzere tüm çıkar sahiplerini ve bağımsız denetçileri derinden etkilemiş, yasaya tabi tüm şirketler finansal raporlamaya yönelik iç kontrollerinin iyileştirilmesi için kapsamlı projeler başlatmışlardır.

Sarbanes Oxley Kanunun Amaçları

Mevcut genel kabul görmüş muhasebe ilkelerinin farklı yorumlara yol açması ve yetersiz kalması dolayısıyla Sarbanes Oxley Kanunu ile muhasebe standartlarını tekrar düzenlemesine ihtiyaç duyulmuştur.

Sarbanes Oxley Kanununun birincil amacı Enron, Xerox gibi ABD'de yaşanan denetim ve muhasebe skandallarının ardından kamunun güveninin tekrar kazanılmasıdır. Bu

kanun ile kurumsal yönetimin şirketler tarafından uygulanmasını zorlamak ve şirket şeffaflığını arttırmak amaçlanmıştır (Cripps, 2002).

Kanununun yürürlüğe girmesi ile niyetlenilen diğer amaçlar şunlardır; (Özeke 2004)

-Yatırımcıya doğru, zamanında, detaylı ve anlaşılabilir finansal bilgi sunulmasının sağlanması,
-Daha iyi kurumsal yönetimin sağlanması,
-Muhasebe Gözetim Kurulu (Public Company Accounting Oversight Board)'nun kurulması ile daha sıkı yaptırımların sağlanması,
-İç kontrollerin daha etkin yapılmasının sağlanması.
-Dış denetim firmaları tarafından desteklenen ve iç denetimden sorumlu denetim komitesinin, bağımsız hareket etmesinin sağlanması. (Denetim Komitesi, bağımsız denetçilerin bağımsızlığını destekleyen ve onlara bu konuda yardımcı olan, bunun yanında işletmenin iç kontrollerini ve dış finansal raporlama sürecinin izlenmesinden sorumlu olması amacıyla seçilmiş bir idari komisyondur (Alvin, 1997).
-Denetim yapan denetçi firmalardan alınabilecek diğer hizmetleri sınırlandırmak amaçlanmıştır.

Sarbanes Oxley Kanununun Türkiye'ye Etkisi

Türkiye, Enron, Xerox ve Worldcom vakalarını yaşamamak için başkalarının tecrübesinden faydalanmayı başarmıştır. Sermaye Piyasası Kurulu (SPK) Sarbanes Oxley Kanununun hükümlerini, SPK'nın seri X No: 16 tebliğinde 02.11.2002 tarihinde Seri: X No:19 Sermaye Piyasasında bağımsız denetim hakkında tebliğde değişiklik yapılmasına dair tebliğinde yapılan değişikliklerle Türkiye'de uygulamaya geçirmiştir

Türkiye'de kurumsal yönetim konusuna yeterince değinilmediği için denetim firmalarının seçiminde bu güne kadar doğal olarak fiyat unsuru öne çıkmıştır. SPK'nın Seri X No:19 tebliği çıkarmasındaki esas amaçlarından biri de kurumsal yönetim konusunu hayata geçirmektir. Ancak, denetimden sorumlu komitenin yine eskiden olduğu gibi fiyat faktörü ön planda tuttuğu sürece bağımsız denetimin işlevi ve yararı ortaya çıkmayacak, getirilen tüm uygulamalar faydalı olamayacaktır (Erdikler, 2003).

5.1.2 COSO

COSO, the Committee of Sponsoring Organizations of the Treadway Commission olarak bilinen Sahte Mali Raporlama Ulusal Komisyonu, 1985'de 5 kuruluş tarafından finansal raporlamanın kalite ve standartlarını geliştirmek amacıyla oluşturulmuş bir özel sektör inisiyatifidir. COSO temelde National Commission on Fraudulent Financial Reporting adıyla ortaya çıkmıştır. Treadway Komisyonunun en önemli hedefi; sahte mali raporların nedenlerini belirlemek ve meydana gelme olasılığını azaltmaktır. Komisyonunun himayesinde iç kontrol literatürünün yeniden gözden geçirilmesi için bir çalışma grubu oluşturulmuş, sponsor kurumların iç kontrol sisteminin kurulması ve etkinliğinin değerlendirilmesi için genel kabul görecek standartlar belirleyen bir projeyi üstlenmesi kararlaştırılmıştır. Bu amaçla Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (COSO) "İç Kontrol Bütünleşik Çerçeve" raporu nu 1992'de yayımlamıştır. Bu rapor, COSO iç kontrol modeli olarak bilinmektedir.

1992 yılında internal control-integrated framework raporu ile iç kontrolün tanımı ve standartlarını belirlemiş, 2004 yılında "Enterprise Risk Management-İntegrated Framework (Kurumsal Risk Yönetimi- Bütünleşik Çerçeve)" adlı raporu yayınlamıştır. Söz konusu rapor risk yönetimi, iç denetimin etkinliği ve tarafsızlığı gibi konularda kurumlara kaynak teşkil etmekte olup iç denetim organları tarafından yol haritası olarak kabul görmektedir.

COSO modeline göre, iç kontrol üst yönetimden başlayarak tüm kurum çalışanları tarafından uygulanan ve kurumun aşağıdaki hedeflerine ulaşabilmesi konusunda kabul edilebilir bir güvence sağlamayı amaçlayan bir süreçtir. Diğer hedefleri;

- Faaliyetlerin etkinliği ve etkililiği
- Mali raporlamanın güvenilirliği
- Mevzuata uygunluk

ABD Hesap Verilebilirlik Ofisi (GAO) bu hedeflere, varlıkların korunması hedefini de eklemiştir (Bartelink, 2008).

- Beş bileşenden oluşmaktadır ki bu beş bileşen:
  - Kontrol çevresi
  - Risk Belirleme

- Kontrol aktiviteleri
- Gözlem
- Bilgi/İletişim

İç denetimle ilgili standartları dünyada yaygın olarak kullanılmaktadır. Kurumsal risk yönetimi ile ilgili COSO belgesi başarılı bir çerçeve için bir eylem planı oluşturmak üzere gerekli ilk adımları içermektedir. COSO'nun Control Self Assessment (Kontrol Öz-Değerlendirme) gibi bazı yöntemleri Türkiye'deki holdingler ve bankalar tarafından uygulanmaya başlanmıştır (Meriç, 2004).

5.1.3 EU 8. Direktifi

10 Nisan 1984 tarihinde kabul edilen 84/253/ECC sayılı 8. yönerge, muhasebe raporları üzerinde yasal açıdan denetim yapan denetçilerin sorumlulukları ve mesleki standartlarıyla ilgilidir. Bu yönergenin amacı, yasal denetçi olarak çalışan kişilerin gereksinimlerinin karşılanması ve Avrupa Birliğine üye ülkelerde denetime ilişkin düzenlemelerin sağlanmasıdır. AB'ne üye ülkelere 1988 yılına kadar bu yönerge doğrultusunda gerekli düzenlemeleri yapma süresi tanınmış ve yönerge 1 Ocak 1990 tarihinde yürürlüğü girmiştir.

Yönerge ile Avrupa Birliğine üye ülkelerde, işletmelerin finansal raporlarının yasal denetimlerini yürütme ve denetimler ile AB hukukunun gerektirdiği doğrulama derecesinde yıllık faaliyet raporlarının yıllık hesaplara uygunluğunu doğrulama amaçlanmıştır. Holdinglerin konsolide finansal raporlarının yasal denetimlerini yürütme ve bu denetimler ile AB hukukunun gerektirdiği doğrulama ölçüsünde konsolide yıllık hesapların, konsolide faaliyet raporlarına uygunluğunu doğrulama, bağımsız dış denetim kapsamı olarak belirlenmiştir.

Söz konusu denetim işini yapan kişiler, gerçek kişiler olabileceği gibi tüzel kişiliğe sahip denetim firmaları da olabilir.

Yönerge; kapsam, yetkiye ilişkin kurallar, mesleki kurallar, mesleki dürüstlük ve bağımsızlık, açıklık ve son hükümler olmak üzere beş kısımdan oluşmaktadır (Sevim ve diğerleri, 2006).

5.1.4 BASEL II

Ülkelerin Merkez Bankalarının bir araya gelerek oluşturdukları bir kuruluş olan BIS "*Bank for International Settlements* "1974 yılında Basel komitesini oluşturmuştur.
Basel Komitesi 1988 Yılında Basel I standartlarını yayınlamıştır. Bu standartlar bankaların uyması gereken çalışma kriterlerini belirlemektedir. Zamanla mali piyasaların gelişmesi sonucu bu standartlar yetersiz kalmış ve Basel II standartları oluşturulmuştur. Dünya bankacılık sektörü 2004'de Basel II düzenlemesiyle tarihinde yeni bir sayfa açmayı planlamıştır. Amerikan Merkez Bankası önceki Başkanı Greenspan bir demecinde "yüzyılın en önemli ekonomik olayı olarak Basel II'yi" ifade etmektedir. Basel II bankaları, müşterileri, derecelendirme kuruluşları, düzenleyici otoriteleri, ve genel makro ekonomik eğilimleri doğrudan etkilemektedir.
Basel II birbirini destekleyen: asgari sermaye yükümlülüğü, sermaye yeterliliğinin denetimi ve piyasa disiplini olarak üç yapısal bloktan oluşmuştur.

Türkiye'de 2009 yılında uygulamaya geçecek olan Basel II'nin ne olduğu KOBİ'ler tarafından doğru bir şekilde kavranması gerekmektedir. Basel II Standartlarına göre KOBİ'ler işletmelerin çalışan sayılarına göre değil yıllık satış cirolarına göre belirlenmektedir. yıllık satış ciroları 50 Milyon EUR'nun altında kalan işletmeler bu standartlar çerçevesinde KOBİ olarak değerlendirilecektir. Basel II özellikle AB sürecinde de önem arz etmektedir. Sonuç itibariyle, reel sektörün hemen işe koyularak Basel II'nin etkilerini değerlendirip değişimi başlatması gerekmektedir (ATO, 2008).

BDDK tarafından Basel II yol haritasına göre Türkiye için getirilen zorunluluklar bankaların operasyon riskli durumlarını ve zarar olaylarını sınıflandırmalarını, bilgi toplama sistemi geliştirmelerini, ve bunların tutulacağı merkezi bir veritabanını 2004 yılı itibariyle oluşturmalarını öngörmektedir. Kredi riski, operasyonel risk, yapısal faiz oranı riski ve piyasa riski olarak, risk kavramı geniş bir çerçevede ele alındığı standartta asıl amaç bankaların kredi kriterlerinde risk yönetimini ön plana çıkarmaktır.

Basel II'nin Amaçları ; Finansal sistemde güven ve sağlamlığı sağlamak, rekabet eşitliğini artırmak, riskin ele alımında daha kapsamlı ve risk odaklı yaklaşımları ortaya koymak, ve tüm önemli bankalara ulaşacak şekilde sistemi geliştirmektir.

Basel I, piyasa ve kredi riskini temel almaktadır, Basel II'deyse piyasa riski aynen hesaplanmaktadır, ancak buna ek olarak kredi riskinin hesaplanması farklılaştırılmış ve bu risk gruplarının yanına 'operasyonel risk' kavramının eklenmesi gereği görülmüştür.

Basel I'de bütün bankalara tek tip uygulama yapıldığı için risk duyarlılığı istenildiği boyuta ulaşamamış, fakat Basel II ile risk duyarlılığına yönelik hesaplamalar farklılaşmıştır. Basel II'deki en önemli fark, risk ağırlıklarının belirlenmesinde bağımsız derecelendirme kuruluşlarının çalışacak olmasıdır. Ayrıca Basel I'de OECD üyesi ülkelerin hükümetlerine yüzde 0 risk ağırlığı öngörülürken, OECD'ye üye olmayan ülkelere yüzde 100 risk ağırlığı öngörülmüştür. Basel II ile bu durum uygulamadan kalkmıştır. Basel II ile öngörülen riskler için karşılık ayrılmasına ek olarak öngörülmeyen riskler için de asgari sermaye ayrılması istenmiştir. Hedef bankaların denetimine maksimum önemi vermek, risk yönetiminin güçlendirilmesi, piyasa disiplini, kredibilite hesaplamasında standarda ulaşılmasıdır.

Basel II risk yönetimi kültürünün gelişmesine önemli katkıda bulunacaktır. Bankaların müşterileri olan reel sektör firmalarının bu gelişimden etkilenmemeleri düşünülemez. Derecelendirme notu olmayan şirketler açısından büyük bir değişiklik yaratmayacak olsa da yüksek derecelendirme notuna sahip kuruluşlar diğerlerine göre avantajlara sahip olacaklardır. Bu durum kuruluşların kayıt dışılığı azaltması ve kurumsal yönetişimin daha önem kazanmasının yolunu açacaktır (Serim, 2006).

5.1.5 TTK - Türk Ticaret Kanunu Tasarısı

Dünya ekonomisi ile entegre olma, yüksek ve sürdürülebilir büyüme oranları ile ekonomik istikrarın sürekli kılınması hedefi doğrultusunda; şeffaflık ve hesap verebilirlik ilkeleri üzerine kurulu olan yeni Türk Ticaret Kanunu Tasarısı'nın yasalaşmasıyla toplumun tüm paydaşlarının bilgiye erişebilirliği ve çıkarlarının korunması da sağlanacaktır. Türk iş dünyasının rekabet gücünün artmasının yanı sıra ticaret mevzuatının Avrupa Birliği müktesebatına uyumunun sağlanması için hazırlanan bir tasarıdır.

Tasarının kurumsal yönetim yaklaşımı dört ana temel üzerine oturmaktadır.
(1) derinlemesine şeffaflık, (2) adillik, (3) hesap verilebilirlik, (4) sorumluluk. Bu dört ana temel, kurumsal yönetim öğretisinde evrensel niteliktedir (PWC, 2008).

Tasarının özellikle anonim şirketlerde yönetim ve temsil ile ilgili esaslar başlığı altında yönetim kurulunun görev dağılımını düzenleyen 366 maddesinin ikinci fıkrasında yer alan: Yönetim kurulu, işlerin gidişini izlemek, kendisine sunulacak konularda rapor hazırlamak, kararlarını uygulatmak veya iç denetim amacıyla içlerinde yönetim kurulu üyelerinin de bulunabileceği komiteler ve komisyonlar kurabilir hükmü ile kurumsal yönetim ilkelerinde denetim komitesi olarak ifade bulan denetim komitelerinin kurulması konusunda yönetim kuruluna yetki verilmiş ancak bu düzenleme ile belli bir ölçütü esas alan, bir gereklilik ya da zorunluluk öngörülmemiştir.

Ticari ve ekonomik hayattaki gelişmeler ve değişimlerin yarattığı hukuki boşluk ve sorunlara evrensel ölçülerde cevap verecek nitelikte düzenlemeler içeren Türk Ticaret Kanunu Tasarısı'nın; özellikle işletmelerde iç denetim açısından incelendiğinde hükümlerinin yukarıda açıklanan şekilde tasarının sistematiğini bozmadan düzeltilmesi, işletmelerin kurumsallaşmasına çok katkısı olacaktır (Cömert, 2008).

Yeni Türk Ticaret Kanunu'nun getirecekleri;

- Dünya ile paralel kavramlar

  –Uluslararası finansal raporlama
  –Bağımsız denetçilerin denetlenmesi
  –Bağımsız denetim
  –KOBİ'lerde raporlama ve denetim
  – Kurumsal yönetim
  –Risk yönetimi

- Vergi uygulamasında beyanname üzerinde düzeltme
- Denetlenmiş raporların her şirketin web sitesinde yayınlanması zorunluluğu
- Ticari defterlerin TMS/TFRS'lere göre tutulması
- Genel Kurulların karar alma yeteneği açısından denetim raporlarının "olumlu görüş" içerme zorunluluğudur.

5.1.6 AS/NZS 4360 Risk Yönetim Süreci (Avustralya/Yeni Zelanda Risk Yönetim Standardı)

Bu standart Joint Standards Australia ve Standards New Zealand Committee OB-007 tarafından 1999 da geliştirilmiş ve 2004 de güncellenmiştir. AS/NZS 4360 standardı riskleri yönetmede ve belgelemede Dünyanın ilk resmi ve çok güçlü bir standardıdır ve

hala riskleri yönetmedeki nadir standartlardan biridir. Bu standart risk yönetimi için jenerik bir kılavuz niteliğindedir.

AS/NZS 4360 kolay ve esnektir ve risk yönetimi AS/NZS 4360'nın beş basamağını gerçekleştiği sürece toplulukları belli bir risk yönetim metodu için zorlamaz. AS/NZS 4360'nın tekrarlanan beş önemli kısmı:

İçeriği saptamak : Ele alınan risklerin saptanması diğer bir deyişle hangi niteliklerin/sistemlerin önemli olduğunu belirlemek

Risklerin belirlenmesi : Ele alınan sistemin içinde hangi riskler görülmüştür?

Risklerin analizi: Risklere bakmak ve eğer destekleyici kontroller varsa belirlemek

Riskleri hesaplama : Artan riskleri belirlemek

Riskleri ele alma : Şirketler tarafından seçilen risklerin azaltılması için riskler ele alınırken izlenen metodu tarif etmektir.

AS/NZS 4360 risklerin işlevsel risk stili grubu tarafından yöneltileceğini varsayar, bu topluluk yeterli yeteneklere sahiptir ve risk yönetimi grupları riskleri belirler, analiz eder ve ele alır. Standardın uygun olup olmayacağı durumlar mevcuttur.

AS/NZS 4360, Sarbanes-Oxley uyumu gerektiren organizasyonlar için, risk yönetim metodolojisi olarak iyi çalışır. Aynı zamanda AS/NZS 4360, riskleri yönetmek için ihtimal ve sonuç gibi geleneksel bir yöntem kullanmayı tercih eden organizasyonlar için de iyi çalışır. Dünya çapında birçok risk yöneticisi ve organizasyon AS 4360'e uyumlu bir yaklaşımla çalışmalarını yürütüyor olabilir. Bir Avustralya organizasyonu düzenli esaslarla denetleniyorsa, bu standardı kullanması gerekli olabilir.

AS/NZS 4360 yaklaşımı şirket veya sistematik riskler için teknik risklerden daha iyi çalışır. AS/NZS 4360 tehdit risk modeli yapılı uygulamaları sağlayan metotları ele almaz. AS/NZS 4360 risklerin yönetimi için genel bir çatı (framework) olarak, web uygulamalarının güvenlik risklerini belirten hiçbir yapısal metot sağlamaz.

AS 4360 güvenlik incelemeleri için riskleri sınıflandırabilse de web uygulamalarındaki tehditleri belirten yapısal metottaki eksikliği ile IT'de diğer metotlardan daha az çekici kalır (AS/NZS 4360, 2004).

5.1.7 OECD Kurumsal Yönetim İlkeleri (Principles of Corporate Governance)

OECD tarafından 1999 yılında hazırlanan ve 2004 yılı içerisinde yeniden gözden geçirilerek düzenlenen Kurumsal Yönetim İlkeleri Raporu çerçevesinde kurumsal yönetimi oluşturan dört esaslı unsuru; adillik, şeffaflık, sorumluluk ve hesap verilebilirlik olarak belirlenmiştir (OECD, 2004).

OECD, raporunda, kurumsal yönetimi, "şirketlerin yönlendirildiği ve kontrol edildiği sistem" olarak tanımlayıp ve "şirket yönetimi, yönetim kurulu, hissedarlar ve diğer çıkar grupları arasındaki ilişkiler dizisini içerdiği"ni vurgulamaktadır. Ayrıca OECD ilkelerinde yönetim kurulunun sorumlulukları içerisinde "bağımsız denetim dahil olmakla üzere şirketin muhasebe ve mali raporlama sistemlerinin güvenilirliğini sağlamak ve özellikle risk yönetimi, mali ve operasyonel kontrol sistemleri ve yasa ile ilgili standartlara uygunluğu denetleyen sistemler gibi denetim sistemlerinin işlerliğini sağlamak" maddesiyle denetim ve risk yönetim sorumluluğu da atanmıştır. Risk politikaları da yönetim kurulunun görevleri arasındadır (OECD, 2004).

Ülkemizde kurumsal yönetim'in tanıtılmasında önemli rolü olan TÜSİAD'ın Kurumsal Yönetim En İyi Uygulama Kodu da yine bu dört ilke temel alınarak hazırlanmıştır. Yatırımcılara göre Türkiye'de kurumsal yönetimin yerleşmesi için kamuyu aydınlatma, pay sahiplerinin eşitliği, piyasaya ilişkin düzenlemeler ve piyasanın altyapısı, şirket devirleri (ele geçirmeler) ile ilgili bir piyasanın varlığı, mülkiyet haklarının korunması, etkin kamu yönetimi, krediler hakkında bilgi, menfaat sahiplerinin katılımı ve yönetim kurullarının bağımsızlığı konuları geliştirilmesi gerekli görülen başlıca konulardır. Türkiye'de Kurumsal Yönetim İlkeleri Dünya'da genel izlenen trendle paralel olarak şirketler için bağlayıcı olmamakla birlikte SPK tarafından yayımlanmış bulunan Kurumsal Yönetim İlkeleri Rehberi hazırlanmıştır.

5.1.8 The Combined Code On Corporate Governance

Combined Code, 1998 yılında, İngiltere'de daha önce yayımlanmış üç raporu esas alan yeni bir rapordur. Turnbull Raporu olarak da adlandırılan ve iç kontroller ve risk yönetimi hakkında özel sektör direktörleri için hazırlanmış rehber niteliğindeki rapor, 2003'te revize edilmiştir. İngiltere, Londra borsası şirketlerine yönelik "uygula-uygulamıyorsan açıkla" esasına dayalı Combined Code raporunda Yönetim Kurulu

Başkanı'nın ücretlendirme komitesinde yer alması konusunda sınırlama kalkmış ve yer alan önerilere uyum sağlanması, Londra Menkul Kıymetler Borsasına kote şirketler için zorunlu hale getirilmiştir (Atamer, 2006).

Combined Code, İngiltere'de kurumsal yönetişim konusundaki yaklaşımı yansıtmaktadır. İngiltere'de hisse senetleri Londra Borsası'nda işlem gören şirketlerin 'iyi yönetişim' ilkesine ve bu konudaki mevzuata bağlılığını sağlamak amacıyla "The Institute of Chartered Accountants in England-Wales" (1999) isimli örgüt tarafından "İç Kontrol, Birleştirilmiş Kurallar Üzerine Yönetim Kurulu Üyeleri İçin Rehber" (Internal Control, Guidance for Directors on the Combined Code) başlığıyla yayınlanan bir versiyonu da vardır (Saltık, 2007). Sarbanes-Oxley gibi, bu kılavuz da, tüm iç kontrol çerçevesi üzerine odaklanmıştır. Muhasebe dönemlerinin başlangıcında uygulanan 2006 ve 2008 olarak iki versiyonu mevcuttur (FRC, 2008).

Combined Code Mevzuatı (Çolak, 2008); Londra Borsası kotasyon şartı, yönetim kurulu üyelerinin yarısının bağımsızlığı, yönetim kurulunun kendi öz değerlendirmesi, ayrıntılı ücret politikası oluşturma ve geliştirme, Hesap verebilirlik ve denetim, ve paydaşlarla ilişkiler konularını içerir.

5.1.9 Risk Management Standard

Hazırlanan Risk Yönetim Standardı İngiltere'nin önde gelen risk yönetim organizasyonlarından Risk Yönetim Enstitüsü (The Institute of Risk Management IRM), Sigorta ve Risk Yöneticileri Derneği (AIRMIC) ve Kamu Sektörü Risk Yönetimi Ulusal Forumu (ALARM) kurumlarının temsilcilerinden oluşan ekibin çalışmalarının bir sonucudur. Çalışmalar esnasında risk yönetimi ile ilgili diğer profesyonel organizasyonların da görüş ve fikirleri alınmıştır.

Kullanılan terminoloji, risk yönetimi süreci, risk yönetimi için organizasyonel yapı, ve risk yönetiminin amacı gibi konularda fikir birliğinin sağlanması amacı ile bir standarda ihtiyaç duyulmaktadır. Risk yönetimi amaçlarının gerçekleştirilmesi için birçok farklı yol vardır ve bunların hepsini tek bir belgeye sığdırmak mümkün değildir. Bu nedenle, bu standart çerçevesinde detaylı ve sıkı kurallar koyan bir standart geliştirmek yada sertifikalanabilecek süreçler oluşturmak amaçlanmamıştır. Farklı yollarla da olsa bu standartın farklı parçalarının hayata geçirilmesi ile, şirketler standarda uygun

çalıştıklarını raporlayabilecek düzeye geleceklerdir. Standart, şirketlerin kendi uygulamalarını karşılaştırabilecekleri en iyi uygulamayı sunmaktadır.

Risk yönetimi sadece şirketler ve kamu kurumları için olmaktan öte, kısa veya uzun vadeli herhangi bir faaliyet için kullanılabilir (IRM ve diğ., 2002).

Çizelge 5.1'de tüm bu yasaların karşılaştırılması mevcuttur.

Çizelge 5.1 : Mevzuatların karşılaştırması.

	Odağı	**İçerik**	**Amaç**	**Getirdikleri**	**Etkiledikleri**
COSO (1985)	Hem Risk Yönetimi hem de iç denetim için ayrı çatıları mevcuttur.	- Kontrol çevresi -Risk Belirleme -Kontrol aktiviteleri -Bilgi/İletişim -Gözlem kapsamıdır.	Etkinlik ve operasyonların verimliliği, Finansal raporlamanın güvenilirliği, Yasalara ve düzenlemelere uyumu amaçlar.	Kurumsal risk yönetimi ile ilgili başarılı bir çerçeve için bir eylem planı oluşturmak üzere gerekli ilk adımları içermektedir.	Tüm dünyada etkisini gösterir. Kamu sektörlerini de içine alarak bankacılık ve reel sektörlerin hepsinde uygulanabilir.
SOX (2002)	Denetim ve Kurumsal Risk Yönetimi Odaklı	Risk belirleme, Belirlenen risklere ilişkin kontrolleri dokümante etme ve değerlendirme, Kontrol etkinliği	Kamu güveni, Doğru, zamanlı, detaylı ve anlaşılabilir finansal bilgi, Daha iyi kurumsal yönetimi	-Kurumsal iletişim -Denetim firmalarının düzenlenmesi -Kurumsal Raporlama	ABD başta olmak üzere tüm ülkelerdeki reel ve finans sektörlerini etkiler.
EU 8. Direktifi (1984)	Muhasebe raporları Denetimi	Kapsam, Yetkiye ilişkin kurallar, Mesleki kurallar, Mesleki dürüstlük ve bağımsızlık, Açıklık ve Son hükümleri kapsar	Yasal denetçi olarak çalışan kişilerin ihtiyaçlarının karşılanması ve denetime ilişkin düzenlemeleri sağlamayı amaçlar.	AB hukukunun gerektirdiği doğrulama ve finansal raporlarının yasal denetimleri getirmiştir.	Almanya, Avusturya, Belçika, Çek Cum.., Danimarka, Estonya, Finlandiya, G.Kıbrıs, Hollanda, İngiltere, İrlanda, İspanya, Portekiz , Slovakya, İtalya, Letonya, Litvanya, Lüksemburg, Macaristan, Yunanistan, Polonya , Slovenya Fransa, Malta, İsveç
TTK (Tasarı)		Şeffaflık, adillik, hesap verilebilirlik, sorumluluk Bilgiye erişebilme ve toplum çıkarlarının korunmasını	-Rekabet gücünü artırmak -Ticaret mevzuatının Avrupa Birliği müktesebatına uyumunu sağlamak	Dünyaya paralel kavramlar, Uluslararası finansal raporlama, Beyannamelere düzeltme, Raporları web sitesinde yayınlama zorunluluğu	Türkiye kamu ve özel sektörü
AS/NZS 4360 (1999)	Risk Yönetimi odaklı	İçeriği saptama, Risk belirleme, Risklerin analizi, Risk hesaplama, Riskleri ele alma konularını içerir.	Risk Yönetim sistemi kurmak ve devamlılığı için sistematik yöntemler sunma	Riskleri yönetme ve belgeleme	Avustralya/Yeni Zelanda

Çizelge 5.1 : Mezuatların karşılaştırılması (devam).

	Odağı	İçerik	Amaç	Getirdikleri	Etkiledikleri
OECD Kurumsal Yönetim İlkeleri (1999)	Kurumsal Yönetim	Kurumsal yönetim, İnsan kaynakları, Süreçler, Örgütsel yapı, İlkeler ve araçlar arası ilişkiler, İşbirlikleri, Strateji belirleme, ve kontrol, konularını kapsar.	Adillik, şeffaflık, sorumluluk ve hesap verilebilirlik esas amaçlarıdır.	Kurumsal yatırımcılara, şirket yönetim düzeyi, yönetim işlevleri, kurumsal iç denetim mekanizmaları ve mali boyutsuz verileri de içeren yönetim uygulamalarını getirmiştir.	Avusturya, Belçika, Kanada, Danimarka, Lüksemburg, Hollanda, Norveç, Portekiz, Fransa, Almanya, Yunanistan, İspanya, İsveç, İsviçre, Türkiye, Birleşik Krallık, ABD, İzlanda, İrlanda, İtalya, Meksika, Yeni Zellanda, Polonya, Slovakya, Güney Kore, Avustralya, Çek Cumhuriyeti, Finlandiya, Macaristan, Japonya
Combined Code On Corporate Governance (1998)	Kurumsal Yönetim altında İç kontroller ve risk yönetimine odaklı	Yönetim kurulu üye bağımsızlığı ve kendi öz değerlendirmesi, Ücret politikası oluşturma ve geliştirme, Paydaş ilişkilerini, hesap verebilirliği ve denetimi kapsar.	'İyi yönetişim' ilkesine ve bu konudaki mevzuata bağlılığını sağlamak amaçlıdır.	Yönetim Kurulu Başkanı'nın ücretlendirme komitesinde yer alması konusunda sınırlama kalkmış ve yer alan önerilere uyum sağlama, zorunluğu gelmiştir.	İngiltere Londra borsası şirketlerine yönelik
Risk Management Standard (2002)	Risk Yönetimi Odaklı	Risk değerleme, risk analizi (belirleme, tanımlama, tahmin) risk yönetim aksiyonu ve süreci, risk raporlama, iletişim, politika, rol ve sorumluluklar	Kullanılan terminoloji, risk yönetimi süreci, risk yönetimi için organizasyonel yapı, ve risk yönetiminin amacı, konularda fikir birliği sağlama	Şirketler standarta uygun çalıştıklarını raporlayabilecek. Şirketlerin kendi uygulamalarını karşılaştırabilecek düzeye geleceklerdir	İngiltere kamu ve özel sektörü
BASEL II (2004)	Risk Yönetimi odaklı	Asgari sermaye yükümlülüğü, Sermaye yeterliliğinin denetimi, Piyasa disiplini	-Finansal sistemde güven ve sağlamlık -Rekabet eşitliği -Daha kapsamlı ve risk odaklı yaklaşımlar	Kurumsal yapılanma, Uluslararası standartlarda muhasebe kayıtları, Kayıt dışı azaltılması, Para ve Risk Yön.	Bankalar, Müşteriler, Derecelendirme kuruluşları, Düzenleyici otoriteleri, ve reel sektörü de etkiler.

5.2 Standard &Poor's derecelendirmesinde KRY kriterleri

Etkili bir kurumsal risk yönetimi yaklaşımına sahip olmak, şirketlerin alacakları derece puanları üzerinde çok olumlu bir etki yaratabilmektedir. Bu amaçla derecelendirme kriteri bir yasa olmasa da önemli görülen bir gelişme olarak bu bölümde anlatılacaktır.

7 Mayıs 2008'de Standard&Poor's kredi derecelendirme kuruluşu finansal olmayan kurumlar için Kurumsal Risk Yönetimi - KRY (Enterprise Risk Management - ERM)

kriterlerini kritiği ile derecelendirme analizini genişleteceğini resmen bildirmiştir. KRY yapılanmasına sahip olmayan şirketler notlarının düştüğünü görecektir. 2004 yılından beri bankalar ve sigorta şirketleri için kullanılan yaklaşımı model alacak olan S&P'un yeni kategorisi, KRY operasyonlarının kalitesini değerlendirmek için yüz civarında farklı faktör kullanacak ve sonra da bu değerlendirmeyi son notu verirken dikkate alacaktır. S&P bu teşvik ile genel olarak yönetim analizini geliştirmeyi, kurumların zorluklara karşı farklılaşmış yeteneklerini belirlemeyi, ve geleceğe yönelik derecelendirme yapmaya yardımcı olmasını beklemektedir. S&P çalışmalarına, finansal hizmetlerden sonra KRY'de en aktif sektör olan enerji sektörü ile 12 petrol ve elektrik şirketi ile pilot programa başlamıştır.

Risk yönetimi, Standard& Poor's'un sigorta ve reasürans şirketlerine yönelik analizlerinin daima en önemli parçasını oluşturmaktadır. Nitekim S&P, 2005 yılının Ekim ayında sigorta analistlerinin kurumsal risk yönetimine ilişkin değerlendirmelerde bulunabilmeleri amacıyla belirlediği bir dizi kriter açıklamıştır. S&P, o tarihten bu yana, söz konusu bu kriterleri uygulamakta olup, değerlendirme sonuçlarını derecelendirmelerine yansıtmaktadır. Bunun anlamı, risk yönetiminin artık derecelendirme kriterlerinin üstü örtülü bir parçası olmaktan çıkıp, başlı başına ve açık bir değerlendirme konusu haline gelmiş olmasıdır (Reasürör, 2007).

S&P enerji pazarlama ve dağıtım sektörlerinde risk yönetim ilkelerine başvurarak genişlettiği çalışmasında ve finansal sektörde KRY'ne başvurma ile derecelendirmeye değer katmayı amaçlamıştır. Aynı zamanda derecelendirme proseslerinin devamlı gelişmesinin taahhütü olarak görmektedir.

S&P'un KRY çerçevesi, bankaların kredi itibarını belirleyen iyi bir araç olup KRY yeteneklerini de değerlendirecektir. Dünyadaki son olaylar bazı savunmasızlıkları doğrulamıştır. Şu anki kredi çevresinde, Standard & Poor's KRY'nin finans dışı firmalarına girmesinin tam zamanı olarak düşünmüş, bir çok firma potansiyel stres altında iken kurumsal risk yönetimini araştırmaya imkan verdiğini belirtmiştir.

Kurum KRY kriterlerini tüm sektörlerdeki firmaların proseslerini derecelendirme de kullanacağını ve bu yayılmanın gelecek aylarda ilerleyeceğeni belirtmiştir. (Standard& Poor's, 2008).

6. KURUMSAL RİSK YÖNETİMİNİN BAŞLICA YÖNETİM YAKLAŞIMLARI İLE İLİŞKİSİ

Günümüzde işletmelerin kontrol ve idaresinde meydana gelen temel değişiklikler oldukça şaşırtıcı yönlerde gerçekleşmektedir. Örneğin, risk yönetimi konusu son otuz yıldır genel itibariyle sigorta kapsamında dikkate alınmıştır. Artık KRY kurumsal yönetimle birlikte ve birbiriyle ilişkili olarak ele alınmaktadır. Aslında kurumsal yönetimin stratejik planlama, risk yönetimi ve iç kontrolden ayrılması yakın zamanlarda gerçekleşmiştir. İşletmeler meydana gelen bu önemli değişikliklerin kendilerini nasıl etkilediğini, risklere dair stratejik şekilde yaklaşabilirliklerini ve planlama süreçlerini ne şekilde değiştirmeleri gerektiğini dikkate almalıdırlar. Bu noktadan hareketle, çalışmanın bu bölümünde KRY'nin stratejik yönetim, değer yönetimi, kurumsal yönetim, performans yönetimi, portföy yönetimi ve iç denetim ile olan ilişkisi anlatılmıştır. Lam, benzer bir ilişkiyi kitabında göstermiş ve belirlemiştir. KRY'i, kurumsal yönetimin temel parçalarından birisi olarak kabul etmiştir.

KRY temel olarak bu yönetim yaklaşımlarının amaçlarının başarılmasında temel unsur olarak gerekli ve önemli olmakla birlikte, aslında KRY ile bu yaklaşımlar arasında iki yönlü bir etkileşim ve ilgi söz konusudur. Ayrıca KRY herhangi bir yönetim yaklaşımı kapsamında değil diğer yaklaşımlar gibi başlı başına bir yönetim yaklaşımı olarak ele alınmaktadır (Küçük, 2007).

6.1 Stratejik Yönetim

Stratejik yönetim, işletmenin gelecekte yer alacağı pozisyonu belirlemeye yönelik süreci kapsamaktadır. Gelecek büyük oranda belirsizlik ve risk içerdiği için KRY'nin

stratejik yönetim çabalarıyla birlikte dikkate alınması ve birbirini destekler şekilde yürütülmesi önem taşımaktadır (Küçük, 2007).

Stratejik yönetimin en sık rastladığımız alanları askeri, ekonomik, siyasal olsa da aslında yaşamın her alanında strateji olgusu karşımızdadır. Kurumlar istediği sonuçlara ulaşabilmek için seçimler yapmak, hedefler koymak, doğru ve yeterli kaynakları bulmak ve doğru zamanda kullanmak isterler ve bunları stratejik yönetim ile uygularlar.

Etkililik ve işlevselliğin sağlanması için risk yönetiminin kurumun faaliyetlerinin ayrılmaz parçası olarak düşünülmesi, stratejik ve yönetsel süreçlerde yer verilmesi esastır. Karar alma, stratejik yönetim ve operasyonel süreçlere entegre edilmiş bir risk yönetimi kurumların yönetim kalitesinin artırılmasının temel taşıdır (TBB, 2006). Çünkü risk kurumun amaçlarını başarmasını, stratejilerini başarılı yönetmeyi engelleyebilecek tehdit olarak adlandırılır (SGUL, 2007).

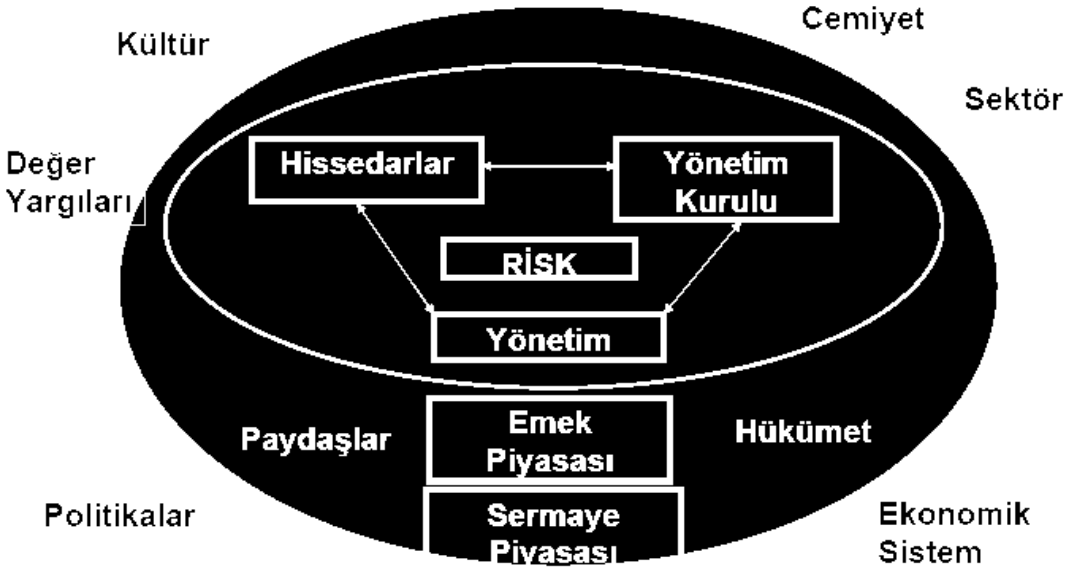
Stratejiler sonuçları etkili ve riskli olabilen seçimlerdir. Stratejik yönetimin özgün yaklaşımı stratejik karar verme sürecine öncelik tanımasıdır. Diğer karar süreçlerinden farklı olarak stratejik kararlar uzun dönemleri kapsarlar, sonuçları risklidir ve işletmenin tümünü ilgilendirir. Bu açılardan KRY ile paralellik göstermektedir.

Bir işletmenin rekabet stratejisi onun riski nasıl gördüğünü ve ne şekilde ele aldığını da belirtmektedir. İşletmelerin bazılarında risk almaya karşı bir tutum olabilirken diğerlerinde riskleri rekabet avantajı sağlamak için alma yönünde bir tutum sergilenebilmektedir. KRY uygulamalarının stratejik yönetim çabaları ile ilişkilendirilmesi ve birbirini destekler şekilde yürütülmesi önem taşımaktadır (Murphy ve Davies, 2001). Bazı firmalarda kurumsal risk yönetimi uygulaması, stratejik yönetim çatısı altında dahi yürütülebilmektedir.

İşletmelerin risk iştahı ve risk toleransı onun stratejik yönetim yaklaşımı ve geliştirdiği stratejiden etkilenmektedir. İşletmenin içinde bulunduğu endüstrinin ve pazarın şartları, örgütsel kültürü ve diğer dış faktörler de risk toleransını etkilemektedir. Risk büyüklüğünün anlaşılması ve belirlenmesi, kaynak paylaşımı ve diğer yönetim seçimlerine etkisi olacak risklerin belirlenmesi için önemli bir noktadır (Küçük, 2007).

6.2 Kurumsal Yönetim

Kurumsal Yönetim (KY) gerekli kontroller ve dengelere dair temel ve geliştirilebilir bir yapı yoluyla işletmelere yardımcı olmaktadır. KY, işletmelere ortakları ve işletme ile ilgili tüm tarafları ile birlikte bugünün hızla değişen düzenlemeleri, piyasalar, finansal ve iş baskılarından kaynaklanan riskleri ve zorlukları yanıtlamalarında en iyi anlayışı, plan ve yönetim faaliyetlerini gerçekleştirme fırsatı vermektedir. KRY ve KY arasındaki ilişki, yönetim kademeleri olarak Şekil 6.1'de gösterilmektedir. Buna göre işletmeler yönetişim faaliyetleri kapsamında amaçlarının, tutumlarının, politikalarının ve risk iştahının belirlenmesine ilişkin çalışmalar yapmaktadırlar. Bu çalışmalar KRY kapsamındaki çabalarla desteklenmektedir. Çünkü KRY'de yönetimsel faaliyetlere ilişkin risklerin belirlenmesi ve analizi yapılmaktadır. Ayrıca bu risklere ilişkin yanıt stratejilerinin geliştirilmesi ve yapılacak kontrollerin saptanması da KRY kapsamında gerçekleştirilmektedir. KY ve KRY faaliyetlerinin uyum çabalarını da dikkate alması gerekmektedir. Amaçlar doğrultusunda ilgili yasa ve düzenlemeler ile uyumlu hareket edilmesi ve ortak beklentilerine karşılık verilerek onlarla iletişim kurulması önemli bir noktadır (Küçük, 2007).



Şekil 6.1 : Kurumsal yönetim ve kurumsal risk yönetimi ilişkisi (Kazmirci ve Altunay, 2004).

Bugünün karmaşık kurumlarında birçok zorluk bulunsa da bunlardan üçü öne çıkmaktadır: kurumsal yönetim, hedef belirleme ve bunlara ulaşılıp ulaşılamadığının bilgisine sahip olma; risk yönetimi, bu hedeflerle ilgili risklerin nasıl yönetileceğinin belirlenmesi, ölçülmesi, raporlanması ve seçilmesi ve raporlama, mevzuata yönelik uygulamaların doğru ve açık gerçekleştirilmesidir. Etkili KY, risk yönetimi ve raporlama, hissedar değerine büyük ölçüde katkıda bulunup bir kuruma (PWC, 2008):

- Risk ve fırsatlara ilişkin daha açık ve geliştirilmiş stratejik iş kararlarının verilmesi,
- Operasyonel sürprizlerin etkin ve aktif gözlemlemeyle en aza indirilmesi,
- Olumsuz olayların gerçekleşme ihtimalinin azaltılarak ve fırsatlardan olabildiğince yararlanılarak marka ve şirket itibarının korunup geliştirilmesi,
- Daha etkin uygulamalarla kurumsal verimliliğin artması, konularında yardım eder.

6.3 Değer Temelli Yönetim

Her şirketin amacı değer yaratmaktır. Risk yönetimi, değerin yaratılmasının, yaratılan değerin korunmasının ve geliştirilmesinin güvencesidir Risk yönetim organizasyonu, şirket üst düzey yönetimi için güç ve görüş kabiliyeti sağlayan ve açıkça değer yükselten bir yapıya sahip olmalıdır.

İşletme liderleri ortak değeri yaratmanın yeni yollarını aradıkları için, değer yaratma ve KRY arasında bir bağlantı keşfetmişlerdir. Liderlerin birçoğu risklerin sadece önlenmesi/kaçınılması gereken bir tehdit olmadığını fark etmişlerdir: risk fırsat yaratır, fırsat değer yaratır ve değer nihai olarak ortak refahı yaratır. Burada önemli soru, risklerin değer oluşturmak üzere nasıl en iyi şekilde yönetileceğidir. Bu sorunun yanıtı ise KRY'dir (Murphy ve Davies**,** 2001).

Vizyonun net olarak ifade edilmesi değer yaratır. Neler bilindiğini anlamak, değer yaratılması ve risklerin en aza indirilmesinde önemlidir. Net bir anlayışın oluşturulması güç olabilir. Ancak değişimin hızı arttıkça, iş modelleri daha da karmaşıklaşmakta ve kurumlar strateji uygularken üçüncü şahıslara daha bağımlı olmaktadır (PWC, 2008).

Değer temelli yönetim (DTY), işletmelerin finansal sonuçlarına dair muhasebe işlemlerinden ve kapital yönetiminden çok daha fazlasını temsil etmektedir. Bu,

yönetimde kararların önceliklerine göre sıralanmasını ve kararların kurumsal değere nasıl katkıda bulunacağının anlaşılmasını öğretir. Ayrıca bütün riskler aynı ölçüde değer yaratmazlar. Riskler değer katkılarına göre dikkate alınırlar. Doğru DTY, stratejik planlama, finansal raporlama, ücret planlama gibi kurumsal faaliyetlerle bağlantı sağlayarak faaliyetleri sıraya koyar (Küçük, 2007).

Yönetimin amacı, işletmenin stratejisini uygulamak yoluyla değeri maksimize etmektir. Bu amaç KRY'de de vurgulu şekilde belirtilmektedir. Analistler, yönetim kurulları ve ortaklar gibi çeşitli çevreler ortak değerini artırmak için yönetim üzerinde büyük baskı yaratırlar. Ek olarak bu baskı, yatırımcılar ve onların acentelerinden de gelir. Değeri yönetmek için çok sayıda geçerli ve iyi neden vardır (Knight, 2003).

DTY kapsamındaki üç unsur onun KRY ile ilişkisinin anlaşılması için yararlı olacaktır. Bunlar; yaratılan değer (maksimum gelecek değeri yaratmak ve artırmak için yöntemler); değerin yönetilmesi (yönetişim, değişim yönetimi, örgütsel kültür, iletişim, liderlik) ve ölçülen değer olarak belirlenmiştir.

Ayrıca DTY aşağıdaki konularda istikrar sağlamayı amaçlar ki bunlar da KRY ile paralellik taşımakta ve DTY'yi KRY ile ilişkilendirmektedir (VBM, 2005);

- Kurumsal misyon (işletme felsefesi) ve stratejii
- Kurumsal yönetim ve organizasyon,
- Örgütsel kültür ve iletişim,
- Kurumsal süreçler ve sistemler kararı,
- Performans yönetim süreçleri ve sistemleri,
- Ödül süreçleri ve sistemleri,
- Kurumsal amaç ve değerdir (normal olarak maksimize edilmiş ortak değeri).

6.4 Portföy Yönetimi

Portföy yönetimi, yatırımcı birikimlerinin, esas değerini koruyacak ve zaman içinde artarak yatırımcının risk beklentileri doğrultusunda yeterli bir getiriyi sağlayacak şekilde yönetilmesi sanatıdır. Sermaye kazançlarının arttırılması için arayışlar her zaman başarıyla sonuçlanmayabilir, bu da kaçınılmaz olarak birikimleri kaybetme riskini beraberinde taşır. Yüksek getiri genelde riski daha yüksek yatırım araçlarıyla ilişkilendirir (Oyak, 2005).

Burada temel soru, "tüm kurum çapında portföyün optimizasyonunu sağlamak için, mevcut yatırımların ve yatırım fırsatlarının nasıl yönetilmesi gerektiği"dir. Yönetimin nihai amacı, ortak değerini en büyükleme (maksimize etme) olduğu için, kurum çapında Portföy yönetimi için temel prensip, iş portföyünü yönetmek olmalıdır. Bu bir fon yöneticisinin stok portföyünü yönetmesiyle aynı yöntemdir. Diğer bir deyişle, portföy yöneticileri risk meydana gelme merkezi ile risk transferi arasındaki bağlantıyı anlamaya çaba harcarlar ve en iyi şekilde kurumsal portföy pozisyonunda yatırım kararı vermeye çalışırlar (Lam, 2003).

Portföy Yönetimi, KRY'yi dört önemli yoldan desteklemektedir. Bunlar; (Lam, 2003)

i. Riskin meydana gelme yeri, alınması ve transfer edilmesi arasında bağlantının oluşturulması (ayrıştırma yapılması),

ii. İşletme çapında bir risk toplama fonksiyonu sağlaması,

iii. Risk limitlerinin ve varlık tahsisi hedeflerinin oluşturulması,

iv. Yatırım kararlarını etkileme.

6.5 Performans Yönetimi

Performans yönetimi, kurumu ileriye götürecek amaçların oluşturulmasını, kaynakların dağılımını ve öncelikli alanlara tahsisini sağlayarak uygulanan politikaların belirlenen amaçlara ulaşmayı sağlayıp sağlamayacağını kontrol eden ve kurumsal kültür ile kurumsal sistem ve süreçler üzerinde olumlu etkiler meydana getirmek üzere performans bilgisini kullanan bir yönetim sistemi olarak tanımlanmaktadır. Performans yönetimi, amaç ve hedeflerin belirlenmesini, performansın ölçülmesini, değerlendirilmesini ve raporlanmasını içeren geniş bir kavramdır. Kurumsal performans yönetiminin uygulanması ile kurumlarda performansı ölçme ve degerlendirme kültürü oluşacak ve bireysel performans yönetimini uygulamak daha kolay olacaktır.

Yönetimin bütün kademelerinde gerçekleştirilen faaliyet ve işlemlerin planlanması, uygulanması ve kontrolü aşamalarındaki etkililiğin, ekonomikliğin ve verimliliğin değerlendirilmesi ile performans odaklı bir risk yönetimi gerçekleştirilebilir.

Yeni yönetim felsefesi anlayışı ile gelen stratejik yönetim, risk yönetimi, performans yönetimi, iç kontrol yönetimi ve yönetişim sistemlerini yönetim ve organizasyon yapısına hızla adapte etmek başarılı bir yönetim için zorunlu hale gelmiştir (Sanayi, 2008).

6.6 İç Denetim ve Kurumsal Risk Yönetimi İlişkisi

COSO tarafından 2004 yılında yayınlanan kurumsal risk yönetimi çerçevesinin yayınlanması ile beraber iç denetim faaliyetlerinde kurumsal risk yönetimi çerçevesi dikkate alınır hale gelmiştir. İç denetim ve KRY içe geçmiş uygulamalar olup aralarındaki ilişki ve görev ayrılıklarını anlamak için bu bölümde konu alınmıştır.

6.6.1 İç denetim nedir?, ne yapar?

COSO'ya göre iç kontrol**;** İşle ilgili hedeflere ulaşmak için kabul edilebilir güvence sağlamaya yönelik süreçlerdir.

Bu tanım çok kısadır, daha öğretici ve kapsamlı bir tanım olarak İç Denetçiler Enstitüsü (The Institute of Internal Auditors) Yönetim Kurulu'nun 26 Haziran 1999 tarihinde kabul ettiği haliyle 'iç denetim'in tanımını vermek daha açıklayıcı olacaktır.

"İç denetim bir organizasyonun operasyonlarının etkinliğini artırmak, iyileştirmek, onlara değer katmak üzere tasarlanmış, nesnel ve bağımsız bir güvence ve danışmanlık sağlama faaliyetidir. Bu faaliyet, yönetim, kontrol ve risk yönetimi süreçlerinin etkinliğinin ölçülmesini ve iyileştirilmesini sağlayacak sistematik ve disiplinli bir yaklaşım getirmek suretiyle, bir örgütün hedeflerini gerçekleştirmesine yardımcı olur."

İç denetim operasyonel faaliyetler ile yönetsel faaliyetleri risk odaklı bir yaklaşım ile denetleyerek, yönetimin şirketi belirlenmiş amaç ve hedefler doğrultusunda yönettiğine dair yönetim kuruluna makul güvence sağlar. Ayrıca iç denetçiler kurumsal yönetim ilkeleri olan şeffaflık, sorumluluk, hesap verilebilirlik ve adillik ilkelerini kurum genelinde yaymak, desteklemek ve tanıtmak misyonuna da sahiptir (Kaya, 2008).

Küresel rekabet içinde sürekli büyüme ve gelişmeyi hedefleyen işletmeler, kurumsal yönetim kalitesini sağlamak amacıyla iç denetim faaliyetine ihtiyaç duymaktadırlar. Bu ihtiyacı duyan yönetim, işletmenin ölçek ve faaliyetlerinin türü, sermaye kaynakları ve

risk faktörlerini dikkate alarak iç denetim faaliyetinin nasıl organize edileceğine karar verir. Ülkemizde, BDDK ve SPK tarafından yapılan düzenlemelerle denetim ve denetim komitesi ile ilgili oluşan mevzuat, Kamu Mali Yönetim ve Kontrol Kanunu ile kamu kuruluşlarının iç denetimine ilişkin düzenlemelerle finans, reel sektör ve kamu kuruluşlarında iç denetim faaliyetinin yasal bir gereklilik haline geldiği, bankaların, diğer finans ve reel sektör şirketlerinin, kamu kuruluşlarının yönetim kurulu, üst düzey yönetimleri ile denetim profesyonellerinin rol ve sorumluluklarının arttığı bir dönem başlamıştır. Yasalaşması beklenen yeni Türk Ticaret Kanunu ile birlikte denetim olgusu tüm şirket ve kuruluşları ilgilendiren ve etkileyen bir konu haline gelecektir.

Günümüzde iç denetim anlayışı önemli ölçüde değişmiştir. Daha önceleri eksiklik ve hile bulmaya odaklanan, işlem odaklı iç denetim anlayışı yerini süreç ve verimlilik odaklı bir danışmanlık anlayışına bırakarak risk yönetiminin önemli bir parçası haline gelmiştir. İç kontrolün genel amaçları ise;

- İşlemlerin etkinliğini ve verimliliğini artırmak,
- Finansal raporlamanın güvenilirliğini sağlamak,
- Yürürlükteki kanun ve düzenlemelerle uygunluğu sağlamak.
- Şirkete ait herhangi bir özel durum veya bilginin ortaya çıkması durumunda bunun kendilerine ve diğer ilgili şirket çalışanlarına ulaşmasını sağlanmasıdır.

İç denetim yöneticisi, kurumun faaliyetlerini, süreçlerini ve bunlara yönelik riskleri de değerlendirerek, denetim kapsamını belirler ve risk esaslı iç denetim planını hazırlar.

İç denetim faaliyetinin performansının değerlendirilmesinde temel faktör; iç denetimin, işletmenin hedeflerine ulaşması, kurumsal yönetim kalitesinin sağlanması ve işletmenin karşılaştığı risklerin yönetilmesine yardımcı olan iç kontrol sistemine ilişkin görüş ve önerileri ile işletme yönetimine sağladığı katma değerdir (TÜSİAD, 2008b).

Sarbanes Oxley (SOX) 302 Ve 404. Maddeler Uyarınca İç Denetimin Görevleri;

- Takımların ve sorumlulukların belirlenmesi : İç kontrol ortamı ve sistemine aşina olmalıdır.

- İç kontrollerin dökümante edilmesi : İç kontrol sisteminin geliştirilmesi, prosedürlerin oluşturulması, uygulanması, sürekliliğinin sağlanması konularında

sorumludur (Etkili iç kontrol sistemi oluşturmak için COSO standartları önerilmektedir). ABD Sermaye Piyasası Kurulu'na gönderilen raporun kapsadığı döneme ait iç kontrol sisteminin etkinliğini değerlendirmeli ve sonuçları raporlamalıdır.

- İç kontrollerin değerlendirilmesi: Değerlendirme tarihinden sonraki döneme ait kontrol sistemlerini etkileyecek önemli değişiklikleri bildirmelidir. Ayrıca değerlendirme görevinin alt görevleri de şöyledir
    - Dökümantasyon kontrolü,
    - Gerçek bir örnek yardımı ile kontrollerin "varlığını" tespit etme,
    - Eksikliklerin belirlenmesi,
    - İç kontrollerin varlığı konusunda karar verme,
    - Değerlendirmenin sorgulanması.
- İç kontrollerin test edilmesi: İç kontrol sistemine yönelik tüm önemli eksiklikler, zayıflıklar ve hile durumunun tespit edilip edilmediği, ilgili denetçilere ve denetim komitesine açıklanmalıdır. Ayrıca test etme görevinin alt görevleri de şöyledir:
    - Örneklemenin oluşturulması,
    - Kontrollerin test edilmesi,
    - Eksikliklerin belirlenmesi,
    - İç kontrollerin "çalıştığı" konusunda karar verme,
    - Değerlendirmenin sorgulanması.

Yönetimin iç kontrol sistemine ilişkin değerlendirmesi, bağımsız bir denetçi (PwC gibi) tarafından onaylanmalı ve faaliyet raporu ile beraber sunulmalıdır. ABD'de SEC en az üç yılda bir şirket bildirimlerini gözden geçirip, şirketleri denetlemeyi isteyebilir (Karaca, 2007).

6.6.2 Kurumsal Risk Yönetimi ve İç Denetim

İç kontrol, KRY'nin vazgeçilmez bir parçasıdır. Kurumun risk yönetim bakış açısı, sağlıklı bir ifade ve yönetim araçları oluşturarak iç kontrolü de kapsar. Önceki bölümlerde açıklanan olgunluk seviyelerinde bahsedildiği gibi, en temel seviyede iç kontroller ön plandadır (PWC, 2006).

İç denetimin kurumsal risk yönetimi içindeki temel rolü önemli risklerin uygun bir şekilde yönetilmesinin ve ayrıca kurumun iç kontrol sisteminin etkin bir şekilde işlemesinin sağlanmasına yardımcı olmak üzere yönetime kuruluşun KRY faaliyetlerinin etkinliği ile ilgili olarak güvence hizmeti vermektir (COSO, 2004b).

İç denetimin KRY'e uygun olan çekirdek faaliyeti, iç kontrol sistemine uygun yönetilen anahtar iş risklerine yardım sağlayan organizasyonun KRY aktivitelerinin etkinliğinde amaç güvencesi sağlamaktır. IIA, KRY prosesinin her safhasında hangi rollerin iç denetim tarafından kabullenilmesi ve kabullenilmemesini belirtmiştir. Çizelge 6.1 iç denetimin KRY kapsamına dair görevlerini içerir.

Çizelge 6.1 : İç Denetimin KRY Kapsamında Rolleri (IIA, 2004)

Kry Kapsamındaki Temel İç Denetim Rolleri	**Şartlı Olarak Alınabilecek İç Denetim Rolleri**	**İç Denetimin Üstlenmemesi 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 • Risk raporlamasını konsolide etme • KRY çerçevesini yürütme ve geliştirme • KRY'nin oluşumuna öncülük etme • Yönetim kurulunun onayına sunulacak risk yönetimi stratejisini geliştirme	• Risk iştahını 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

İç Denetim Enstitüsü risk yönetiminde temel sorumluluğun yönetimde olduğunu vurgulamaktadır. İç denetçiler yönetimin risklerle ilgili kararlarını yerinde incelemeli yerinde destek olmalı yerinde de risklerle ilgili olarak tavsiyede bulunmalıdır. Ancak risk yönetimine ilişkin kararları bizzat almamalıdırlar. İç denetimin risk yönetimine ilişkin sorumlulukları denetim komitesi tarafından onaylanmalıdır (Sezer, 2005).

Kurumun risk olgunluğu arttıkça ve risk yönetimi iş operasyonları ile daha fazla bütünleşmiş oldukça, iç denetimin kurumsal risk yönetimine destek verici rolü de

azalabilecektir. Aynı şekilde, eğer bir kurum risk yönetimi uzmanı istihdam eder veya risk yönetimi fonksiyonu için uygun bir kadro oluşturursa, iç denetimin, danışmanlık hizmeti vermekten ziyade, güvence verme rolüne odaklanmak suretiyle kuruma katkı sağlaması daha mümkün ve muhtemeldir (Madendere, 2005).

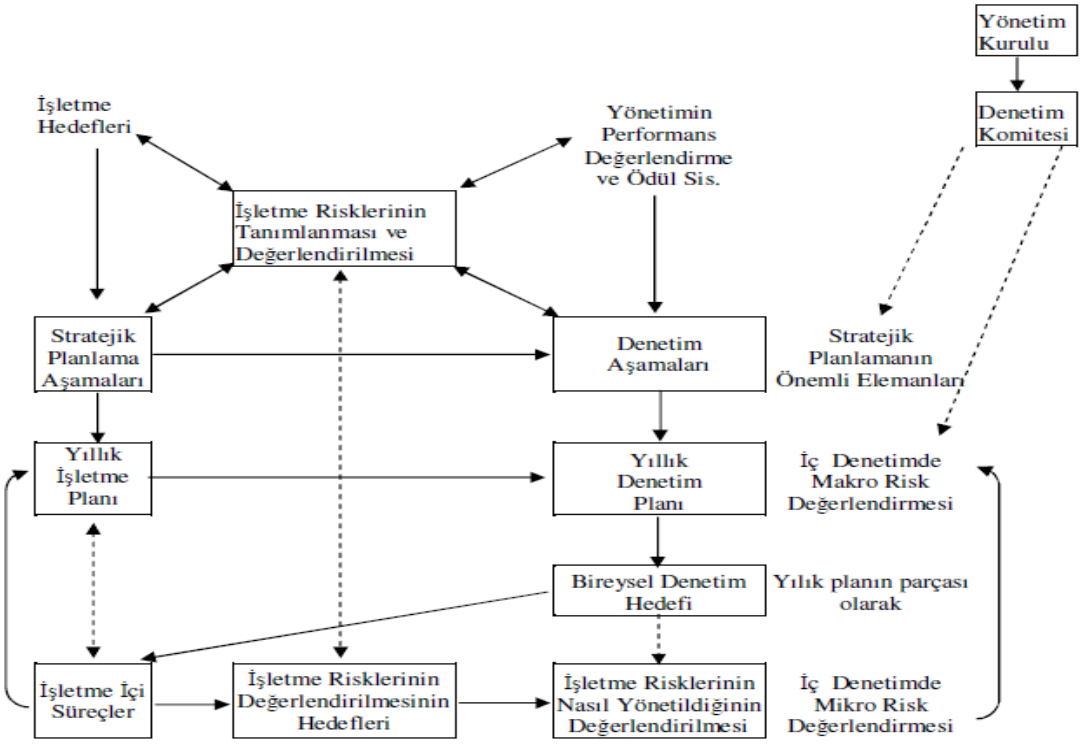
İç denetim, normal olarak, şu konularda güvence sağlayacaktır:

- Risk yönetimi süreçlerinin yapısı/yapılanması ve işleyişi,
- "Temel riskler" olarak sınıflandırılmış olan risklerin yönetilmesi, bu risklerle ilgili kontrollerin ve riskler karşısında alınan diğer tutumların etkililiği,
- Risklerin tam, doğru ve güvenilir şekilde değerlendirilmesi ile risk ve kontrol konu ve durumlarının güvenilir ve uygun şekilde raporlanması.

6.6.3 Risk Odaklı Denetim Anlayışı

Örgütlerde meydana gelen hızlı ve kesin değişmeler risk odaklı iç denetim yönteminin doğmasına zemin hazırlamıştır (McNamee ve Selim, 1998). 1992 yılında COSO tarafından İç Kontrol çerçevesinin yayınlanmasıyla kullanılmaya başlanan "Risk Odaklı İç Denetim" teriminin ve haliyle denetimde risk odağının KRY çerçevesi ile beraber "KRY Temelli İç Denetim" olarak kabul gördüğü bilinmektedir.

İngiltere'deki İç Denetçiler Enstitüsünün Ağustos 2003'te yayınlamış olduğu "Risk Based Internal Auditing" adlı yayında da iç denetimin süreç bazlı denetimden risk odaklı denetime geçtiği ve risk odaklı denetimin hakim yaklaşım olarak kabul gördüğünü, iç denetimin önemli görevlerinden biri olarak kurumun risk yönetimi süreçlerinin denetlenmesinin ön plana çıktığı, iç denetimin yeni tanımına uygun bir denetimin risk odaklı denetim olabileceği belirtilmektedir (IIA-UK, 2003). Şekil 6.2'de Risk odaklı denetimin süreçler arası ilişkisi gösterilmektedir.



Şekil 6.1 : Kurumsal risk yönetimi ve iç denetim ilişkisi (McNamee ve Selim, 1999)

7. KURUMSAL RİSK YÖNETİMİNE GÖRE RİSK İŞTAHI, RİSK TOLERANSI ve RİSK ZEKASI

7.1 Risk İştahı

Risk iştahı, geniş anlamıyla bir değer için bir kurumun almayı kabul ettiği risk oranıdır. Kurumun risk yönetim felsefesini yansıtır ve buna karşılık kurumun kültürünü ve işletme stilini etkiler.

Risk iştahı strateji belirlemede değerlendirilir. Strateji belirlemede, bir stratejiden beklenen gelir kurumun arzuladığı risk oranıyla aynı seviyede olması gerekir. Değişik stratejiler kurumu değişik risk seviyeleri ile karşı karşıya bırakır ve strateji belirlemede kullanılan KRY, yönetime kurumun arzuladığı riske bağlı olarak bir strateji seçmesinde yardımcı olur.

Kurum risk iştahını yüksek, orta, düşük gibi nitelik bakımından veya büyüme hedefleri ve risk getirisini yansıtıp dengeleyerek nicelik bakımından sınıflandırabilir. Risk iştahı daha fazla olan bir şirket, sermayesinin büyük bir bölümünü gelişmekte olan pazarlar gibi daha riskli alanlara yatırabilir. Buna karşın risk iştahı daha az olan bir şirket, kısa dönemde zarar etme riskini azaltmak için olgun ve stabilize pazarlara yatırım yapabilir.

Risk iştahı, kaynakların bölüştürülmesinde de yol gösterir. Yönetim kaynakları bölümler ve teşebbüsler arasında, kurumun risk iştahı ve bölümün yatırılan kaynaktan sağlayacağı getiriyi göz önüne alarak bölüştürür. Yönetim arzuladığı riski, kurumu, insanları ve işlemleri bir araya getirerek değerlendirir ve etkin bir şekilde riskleri izleyip riske karşılık vermek için altyapısını şekillendirir (PWC, 2006).

Risk almaya karar veren ama ne kadar risk almayı kabullenebileceğini bilmeyen şirketin risk alma kapasitesi , şirketin bir defada sermayenin veya mevcut varlıkların ne kadarını riske atmaya ve ileriki dönemlerde büyüyebilmek için ne kadar risk almaya hazır olduğu, büyük bir risk olayı karşısında ne kadar dayanıklı olduğu, akıllıca ve

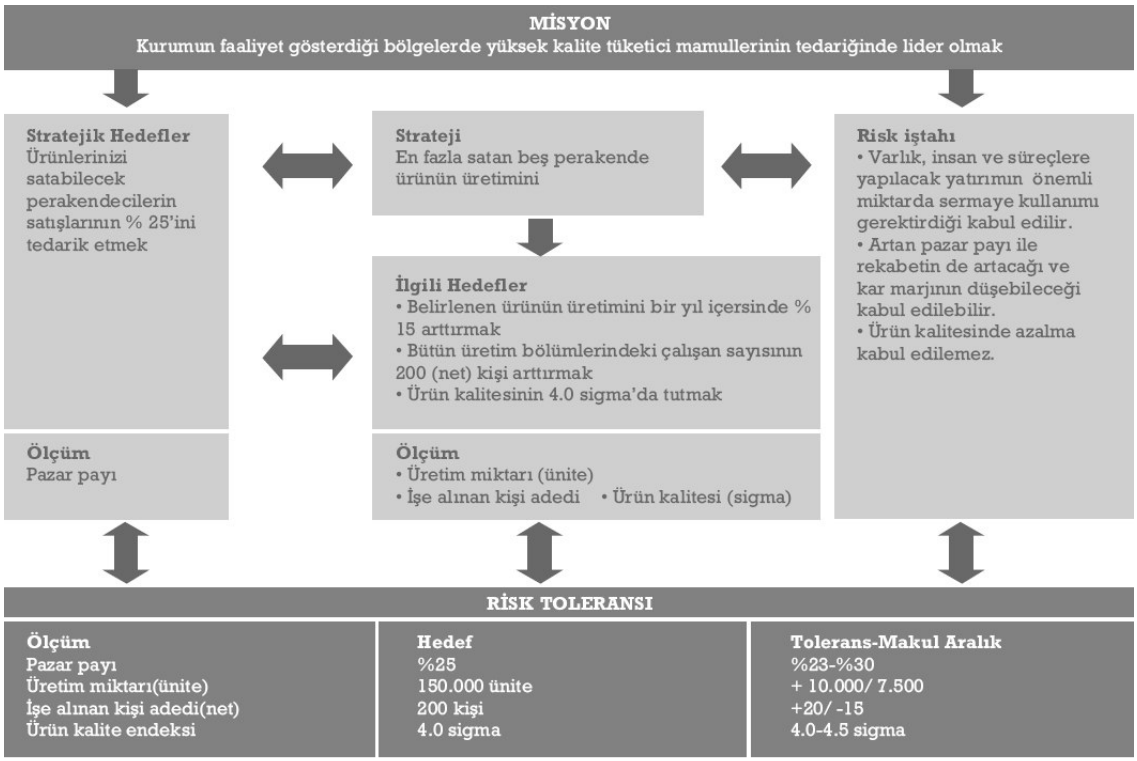
yeterince risk alınıp alınmadığı sorguları risk iştahını belirlemede en önemli yardımcılardır (Deloitte, 2008).

Voltaire'in meşhur sözünden yola çıkarak denilebilir ki **"**Risk, bir teknenin, yelkenini şişiren rüzgara benzer. Fazlası tekneyi batırır. Azı da tekneyi olduğu yerde saydırır.**"**

Voltaire, risk yerine hırsı kullanmıştır arasındaki benzerliği öngörerek sözü yukardaki gibi düzenlemek yanlış sayılmaz. Ve böylece denilebilir ki şirketler başarı sağlamak için risk almak zorundadırlar, ama bu fazla olursa batmalarına sebep olabilir az alırlarsa da ilerleyemez oldukları yerde kalabilirler.

Risk iştahını belirleyen faktörlerin neler olabileceği şöyle sıralanabilir (SGUL, 2007) ;

- Hissedarların beklentileri
- Geçmiş tecrübeler
- Bölümlerin hayatta kalma tehdidine uğraması
- Risk alanlarının doğası (öz faaliyetlerden mi?)
- Kişisel risk iştahı (örn; bölüm başkanı/direktörü gibi)
- Bütün olarak kurumun dışına kontrol kaybetme mesajı



Şekil 7.1: Strateji, Hedef, Risk İştahı Ve Risk Tolerans İlişkisine örnek (İnfomag, 2006).

Şekil 7.1'de strateji, hedef, risk iştahı ve risk tolerans ilişkisi örneklerle anlatılmaktadır. Firmaların risk alma teşvikleri olan CEO'lar la firmaların telafi seçenekleri üzerine kurulmuş, ve aynı zamanda bir CRO kiralamayı olası kılmaktadır. Bu sonuçlar sezgilere aykırı gözükmektedir, fakat CEO'ların risk alma teşviklerine karşın bir kontrol sağlamak için yönetim tarafından bir CRO atanması ile de uygun gözükmektedir (Pagach ve Warr, 2007).

7.2 Risk Toleransı

Risk toleransı, amaçların gerçekleşmesiyle ilgili olarak kabul edilebilir fark düzeyidir. Risk toleransı performans hedefleri yardımıyla ölçülebilir. Performans hedefleri; çoğu kez, amaçların ilişkili olduğu aynı birimlerde ölçülür. Risk toleransları çerçevesinde faaliyet göstermek yönetime kurumun risk iştahı içinde kaldığı ve amaçlarını gerçekleştirdiği konusunda çok daha fazla güvence sağlar (Yörüker, 2007).

Risk toleransının ortaya konulmasında yönetim, ilgili objektifin önemini ve risk iştahı ile orantılanmış risk toleransını dikkate alır. Risk toleransları ile operasyonları

gerçekleştirmek, kurumun risk iştahı sınırında kalmasını ve sonucunda da hedeflediği değerlere ulaşmasını sağlar (PWC, 2006).

Yönetim; riski ele alan çeşitli metotların etkilerini değerlendirmenin ardından risk tolerans sınırları çerçevesinde hem risk olasılığına hem de risk etkisine yönelik olarak tasarlanmış bir cevabı veya cevap kombinasyonunu seçmek suretiyle riskin en iyi nasıl yönetileceğine karar vermelidir. Seçilen cevabın zorunlu olarak, en az miktarda artık risk sonucunu doğurması gerekmez. Ancak, eğer cevap yine de risk tolerans derecesini aşıyorsa, yönetimin ya cevabı ya da risk tolerans düzeyini yeniden incelemesi gerekecektir (Yörüker, 2007).

7.3 Risk Zekası

Risk zekası bir organizasyonun, bir takımın veya bir bireyin öz yetkinliklerindendir. Genel bilgi veya deneyimden daha sınırlı iken, teknik bilgiden biraz daha geniştir. Bir riskin kaynaklarını neler içerebileceğini belirleyebilen birikilmiş bir deneyimdir (Apgar, 2006).

Kurumsal risk yönetimin amacı 'risk zekası' kavramını kuruma aşılamaktır. Risk zekasına sahip kurumlar:

- Risk yönetim uygulamaları bütün kurumu kapsayan, çok çeşitli endüstrilerde faaliyet gösteren çok büyük kurumların farklı iş kollarındaki şirketlerinde oluşmuş risk yönetim silolarının arasındaki bağlantıları kuran;

- Risk spektrumundaki tüm risklere (finansal, operasyonel, stratejik, çevre riskleri gibi) hitap eden risk yönetim stratejilerini bulunduran;

- Risk irdeleme süreçlerinde geleneksel olarak olasılığa verilen önemin yanı sıra 'savunmasızlık' kavramına da büyük önem veren;

- Risk yönetim yaklaşımlarında risk olaylarını sadece birer birer ele almayıp, birden fazla riskin birbirlerini nasıl etkileyeceğini irdeleyen risk senaryoları üreten ve bu senaryolara karşı yanıtlarını planlayan;

- Kurumsal kültüre risk yönetimi kavramını aşılayan ve böylece strateji belirleme ve karar alma süreçlerini riskleri göz önüne alarak yapan; ve

- Sadece risklerden kaçınmaya odaklanmamış, bununla birlikte kuruma değer yaratma adına doğru riskleri doğru zamanlarda almaya odaklanmış risk yönetim felsefesini içeren kurumlardır.

Risk zekasına sahip bir kurum olabilmek uzun ve bazen çok çaba isteyen bir süreç gerektirmektedir. Bu süreç her kurum için kurumun karşılaştığı farklı iş zorlukları ve mevcut risk yönetim becerileri ve yetkinliklerindeki çeşitlilikten dolayı farklı olacaktır. Her ne kadar bu süreç her kurum için farklı olacak ve her kurum bu süreci kendi ihtiyaçlarına göre dikkatlice tasarlayacaksa da risk zekasına sahip bir kurum olabilme süreci genel olarak şu adımları içermelidir (Tekgül, 2007):

- Risk değerlemesi ve yönetimi için kapsamlı çerçeve, politika ve süreç oluşturmak
- Önemli riskleri ve savunmasızlıkları tespit etmek ve yanıtları planlanmak
- Kurumun risk alma isteğini ve kurumun ne kadar risk almış olduğunu belirlemek.
- Risk alma isteği ile mevcut alınmış risk miktarını karşılaştırıp daha fazla risk alabilme ve alınmış riskleri azaltma fırsatlarını ve gereksinimlerini belirlemek
- Kurum adına risk almak için kimin (hangi yönetim birimlerinin ve personelinin) sorumlu ve yetkili olduğunu belirlemek
- Riski entegre ve sürdürülebilir bir şekilde yönetme yetkinliklerini belirlemek

Risk zekasına sahip bir kurum olabilmek için bir kurum yukarıdaki adımları attıktan sonra ise şu mükafatları alacaktır:

- Kritik risk sorunlarının olmasını önlemek, risk sorunları ortaya çıktıktan sonra bunları hızlı bir şekilde tespit edebilmek, oluşacak sorunları düzeltmek, ve ilgili bilgileri kurumdaki doğru yönetim birim ve personeline ulaştırmak ile ilgili gelişecektir.

- Risk yönetim prensiplerini ve dilini standartlaştırarak iş operasyonlarının üzerindeki risk yönetimi ili ilgili yük hafifleyecektir.

- Kurumdaki risk enformasyonunu ortak kullanarak ve mevcut risk yönetim fonksiyonlarını entegre ederek risk yönetimi maliyeti azalacaktır.

- Yönetim kurulu, hissedarlar ve diğer paydaşlara kurumun tüm risklerinin yönetim tarafından doğru anlaşıldığı ve yönetildiği ile ilgili bir güven ortamı yaratılacaktır (Deloitte, 2008).

8. KURUMSAL RİSK YÖNETİMİNİN FAYDALARI, KISITLAMALARI VE BAŞARI FAKTÖRLERİ

8.1 Kurumsal Risk Yönetiminin Faydaları

Kurumsal risk yönetiminin şirkete fayda sağladığı bir çok yerde vurgulanmıştır. KRY bir kuruma, amaç ve hedeflerine ulaşmak üzere risklerini yönetmede çok önemli katkı sağlayabilir. KRY'nin katkısı şu hususlarda gerçekleşir (Madendere, 2005; IIA,: Tusiad 2008a; İnfomag, 2006);

- Kurumsal amaçlara ulaşma olasılığını arttırmak,
- Yönetim seviyesinde farklı risklerin konsolide şekilde raporlanmasını sağlamak,
- Temel riskler ve bu risklerin tüm etkilerinin bilinmesi anlayışını geliştirmek,
- Karşılaşılan iş risklerinin paylaşmak ve belirlemek,
- Yönetimin gerçekten sorun olan konulara odaklanmasını sağlamak,
- Daha az krizler ve süprizler, ve bunlara daha hazır olmak,
- Örgüt için doğru yolda doğru şeyleri yapmaya daha çok odaklanmayı sağlamak,
- Belirsizlikten ve değişkenlikten değer yaratılmasını ve başarıya katkı sağlamak,
- Büyük kazanımlar için büyük riskler alma kabiliyeti sağlamak,
- Etkin karar alma ve risk alma da daha çok bilgi sağlamak,
- Daha yüksek bir risk duyarlılığı,
- Daha güvenilir karlılık tahminleri ve karlılığın artması,
- Daha düşük yönetişim riski,
- Daha iyi ve etkin kaynak dağılımı ve kullanımı,
- Menfaat sahiplerinin güveninin ve itimadının geliştirilmesi,
- Kanun ve mevzuatlara uygunlukda sürekliliğinin sağlanması,
- Performansın risk odaklı takip edilmesi,
- Çapraz iş risklerinin tanımlanması ve paylaşılması,
- Gerçekleşen sorunların çözümüne odaklı yönetim ve daha az zaman harcanması,

- Stratejilerin daha sağlıklı belirlenmesi,
- Yatırımcıların ilgisinin artması,
- Birimler arası iletişimin ve iş birliğinin arttırılması,
- Fırsatların ve tehditlerin daha iyi tespit edilmesi,
- Rekabet gücünün artması,
- Reaktif yönetim yerine proaktif yönetim yapılabilmesi,
- Olayların daha iyi yönetilmesi ve zararlarının azaltılması, dolayısı ile riskin maliyetinin düşürülmesi (sigorta maliyetleride dahil) olarak ifade edilebilir.

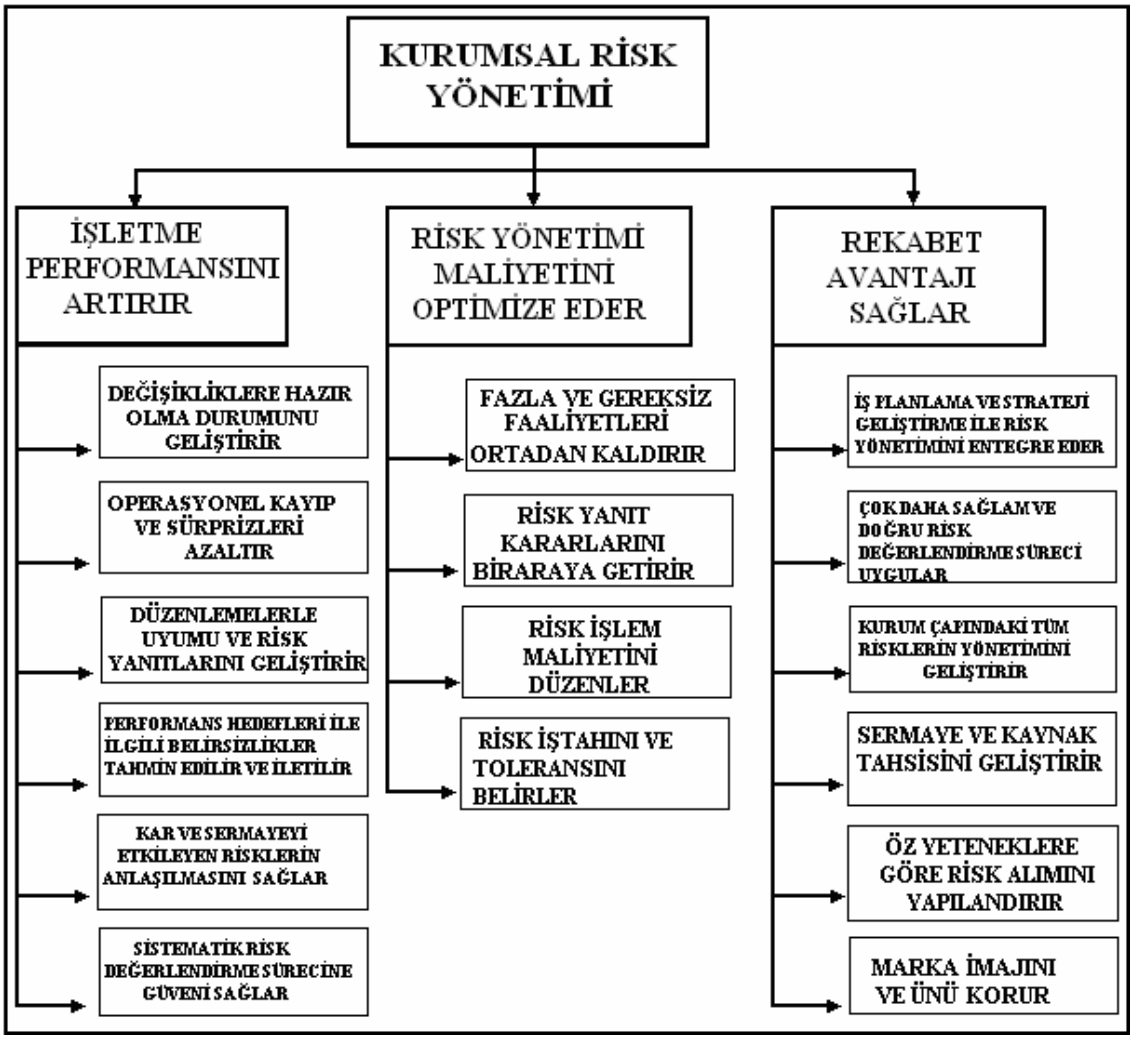
KRY'nin kuruma sağladığı fayda, kurumun özelliklerine ve KRY uygulamalarının etkinliğine son derece bağlıdır. Bu nedenle yukarıda listelenen her bir faydanın her kurumda görülmesini beklememek gerekir. Daha öncede ifade edildiği gibi eğer kurum KRY ile ilgili hedeflerini sağlıklı bir şekilde belirlemiş, sistemini bu hedeflere uygun bir şekilde geliştirmiş ve faaliyetlerini bu sistemlere paralel bir şekilde gerçekleştirmiş ise KRY sisteminden maksimum faydayı sağlayacaktır (TÜSİAD, 2008a).

KRY'nin faydaları yapılan global bir araştırma ile gözler önüne serilmek istenmiştir. PWC'nin 2004 yılında yayımını yaptığı "7th Annual Global CEO Survey" adlı araştırmanın ana konusu Riski yönetmede CEO'ların hazırlıklı olmasına dair bir değerlendirme "**Managing Risk:** An Assessment of CEO Preparedness" dir. Bu araştırma toplam beş kıtada, finansal hizmetler, teknoloji ve medya, tüketici ve sanayi ürünleri ve hizmetleri olarak üç farklı sektörde %33'ünün geliri 1 milyar $'ın üzerinde ve 5000 kişiden fazla çalışanı olan 1400 firmanın CEOları ile görüşleri alınarak yapılan araştırmanın sonuçları %'lik dilimleri ile aşağıda yer almaktadır.

- *Etkin yönetim prosedürlerinin oluşturulmas ı- 47%*
- *Değer yaratacak risklerin alınması - 44%*
- *CEO'ların faaliyetlere olan güveninin artması - 44%*
- *Performansın daha iyi takip edilebilmesi - 44%*
- *Yasal düzenlemelere uygun raporlamanın gerçekleştirilmesi - 41%*
- *Paydaşlara/Hissedarlara gerekli bilgilerin aktarılması - 39%*
- *İtibarın iyileştirilmesi - 38%*
- *Kurum genelinde karar mekanizmaları ve iletişim ağının netleşmesi - 31%*

- *CEO'ların girişimciliğini ve yaratıcı düşüncesini desteklemesi - 30%*
- *Stratejik hedeflere ulaşılması - 28%*
- *Sürdürülebilir karlılığın sağlanması - 28%*

KRY'nin şirketlere değer kattıkları artık konuyla ilgilenen herkesin bildiği bir olgudur. Şekil 8.1'de görüldüğü gibi KRY'nin kurumsal değerleri koruyan ve katkıda bulunan onaltı katma değeri üç ana başlıkta toplamak mümkündür.



Şekil 8.1 : KRY'nin kurumsal katma değerleri (Protiviti 2006b; COSO, 2004a).

8.2 Kurumsal Risk Yönetiminin Kısıtlamaları

KRY uygulamasının çok sayıda faydaları olmasına rağmen, burada dile getirilmesi gereken sınırlılıklar bulunmaktadır. KRY'nin ne denli iyi tesis edildiği ve uygulandığı

ile ilgisiz olarak, KRY işletmenin amaçlarının başarılmasını garanti etmemektedir (Chapman, 2006).

Kurumsal risk yönetimi, yönetime amaçlarına ulaşma çabalarında yardımcı olur. Kurumsal hedeflere ulaşmak yönetim sürecinde var olan bazı sınırlamalardan doğal olarak etkilenir. Devlet politikalarındaki değişiklikler, rakiplerin davranışları veya ekonomik koşullar yönetiminin kontrolü dışında olan unsurlardır (Sezer, 2005).

Risk gelecekle bağlantılıdır. Gelecek, yapısı itibariyle belirsizdir. Bazı olaylar yönetimin kontrolü dışında gelişir. Bu da kısıtlamaların başını çekmektedir.

Etkin KRY bile farklı hedefler doğrultusunda farklı seviyelerde yürütülebilmektedir. KRY, stratejik ve operasyonel hedeflerde yönetimin zamanlı bir şekilde işletmenin hedeflerine ne kadar yakın olduğunu gösterebilmektedir. Ancak, hedeflerin gerçekleştirilebilirliği hakkında kesinlik sağlayamaz. Ancak bunun için makul oranda bir güvence sağlar. Kontrol dışında gelişen bir durum, bir hata, ya da uygunsuz raporlamalar gerçekleşebilir. Yani, etkin bir KRY'de bile hatalar ile karşılaşılabilinir. Bu bağlamda makul güvence, kesin güvence demek değildir (Küçük, 2007).

KRY'nin etkinliği yanlış kararlar verebilen insanlarla sınırlıdır. Kişilerin karar alma biçimleri hatalı olabilir ve basit hata ve yanlışlardan ötürü ciddi sorunlar ortaya çıkabilir. Süreçlerin içinde var olan kontroller iki veya daha fazla çalışanın işbirliği sonu işlemez hale getirilebilir, yönetimin kurumsal risk yönetimini işletmeme, bunun içinde risklere karşı alınan tedbirler de bulunmaktadır (Sezer, 2005). Kararlar, kısıtlı zamanda, mevcut verilerle ve işin doğurduğu baskı altında alınabilmelidir. Kaynaklar sınırlı olduğundan işletmeler kaynaklarının maliyet ve kazanç hesaplarını yapmak zorundadırlar. Kaynaklara ilişkin kararlar risk yönetim ve kontrol faaliyetlerini de içermelidir. Önemsiz risklere gereğinden fazla kaynak ayrılmamalıdır. Gereğinden fazla kontrol, maliyeti yükseltip verimliliği de azaltabilir (Küçük, 2007).

Sonuç olarak kurumsal risk yönetimi yönetime amaçlarına ulaşma noktasında yardımcı olmakla birlikte, her derde deva bir iksir değildir.

8.3 Kurumsal Risk Yönetiminde Başarı İçin Kritik Etkenler

Kurumsal risk yönetiminin tesis edilmesinden uygulanmasına tüm aşamalarında başarılı olması için başta yönetim kurulu olmak üzere tüm şirket çalışanlarının dikkat etmesi gereken hususlar vardır. Bunlar KRY'nin kritik başarı faktörleri adı altında sıralanabilir (Süel, 2001; Saka, 2006; PWC, 2006);

- Yönetim kurulunun ve üst yönetimin desteği ve aktif rol oynaması sağlanmalıdır,
- KRY kavramının oluşmasında ve bunun şirkete katacağı değeri belirlemede gerekli zemin oluşturulması,
- Riskleri yönetmek için sorumlu bir birim oluşturulmalı ve bu birimden sorumlu yönetici belirlenerek görev ve sorumluluklarının açık bir şekilde tanımlanması,
- Tüm risk çeşitleri ele alınması ve tüm risk faktörleri değerlendirilmesi,
- Değerlendirmeye organizasyonun alt seviyelerinden başlanması,
- Risklerin hedefleri nasıl etkilediği üzerine yoğunlaşılması,
- Veri toplanmalı ve modeller oluşturulması,
- Risk değerlendirmelerinde ortaya çıkan bilgilerin uygulanması ve raporlanması,
- Hedef ve stratejilerin net ve anlaşılır bir yaklaşım oluşturularak belirlenmesi,
- Teorik yaklaşımlardan kaçınmak ve işlerin gerçeklerine uygun çözümler üretmek,
- Risk yönetim önerilerinin hayata geçirilmesinde iş birimleri yöneticilerine yardım ,
- KRY'nin tehditler kadar fırsatlara da odaklanması,
- Kurumsal risk profilinin hiçbir soruya neden olmaksızın net bir şekilde bilinmesı,
- Uygulamaların sistematik ve sürekli olmasının sağlanması, kaynakların yeterliliği,
- Orta düzey yöneticiler tarafından anlaşılması ve desteklenmesi,
- Kurumların risk yönetimlerindeki performanslarının genel performans değerlenmesinde önemli bir unsur olması,
- Yeterli düzeyde iletişim kanalları ile eğitim ve iletişim faaliyetlerinde bulunulması,
- Üst yönetimin kurumsal kültürü değiştirme isteği ve gücü,
- Risk yönetim tekniklerini ve iş süreçlerini anlayarak risk yönetim çabalarına liderlik edebilecek kalitede insan kaynaklarına sahip olunması,
- Risk yönetim sürecinin etkinliğini izleme amacıyla denetim mekanizmasının kurulması,

- Çalışanların risk değerleme sürecinin başarısına katkı yapmalarının özendirilmesi,
- Risk yönetim sürecinden kaynaklanan tasarrufların başarılar olarak duyurulması,
- KRY'nin işleyen bir süreç olduğunun ve düzensiz aktivitelerle ve girişimlerle sınırlı olmadığının kabul edilmesi ve tanınması,
- Gelişme ve ilerlemeyi izlemek için iş çıktıları ve fayda ölçümlerini geliştirmek,
- Uygun şekilde kontrol edilen, yönetilen ve doğru nedenlerden kaynaklanan makul proje girişimlerinin planlanması ve uygulanmasıyla oluşan risklerin, şirket bakış açısındaki değişiminin yönetilmesi,
- Organizasyon kültürünün desteklediği sağlam risk yönetimi süreçlerinin ve yapılarının derecesinin değerlendirilmesi,
- Risk, risk yönetimi, KRY ve iç kontrol hakkında ortak tanım ve terminolojinin oluşturulması,
- Önemli KRY kavramlarının ve prensiplerinin işleyen ana iş süreçlerine entegresi,
- Organizasyonun KRY felsefesini, mantıksal temelini, ilintili olduğu konuları tanımlayan, derinlemesine yapılaşmış bir iş konusunun geliştirilmesi,
- Tüm organizasyondan gelen ham veri topluluğunun kontrolü için bilgi yönetiminin kurulması.

Görüldüğü gibi kurumsal risk yönetiminin başarısını etkileyecek bir çok faktör bulunmaktadır. Tüm bu başarı faktörlerinin kurumunun tamamına bildirilmesi de başarıyı etkileyecek en önemli etkendir.

9. DÜNYADA VE TÜRKİYE'DE KURUMSAL RİSK YÖNETİMİ VE FARKINDALIĞINI ÖLÇMEK İÇİN YAPILAN ARAŞTIRMALAR

Hızla popülaritesi artan kurumsal risk yönetiminin Dünyada ve Türkiye'de hangi yöne doğru ve ne hızla ilerlediğini bilmekte fayda vardır. Bu amaçla bu bölümde bu konudaki gelişmeler, uygulamalar ve dünyadaki araştırmaların sonuçlarına bakılacaktır.

9.1 Dünyada ve Türkiye'de Kurumsal Risk Yönetimi

Dünyada ve Türkiye'de Genel Durum

Tüm ülkelerde libarelleşme etkisini hızla gösterirken büyümeyi engelleyici duvarlar kalkmıştır. Yabancı yatırımın nerdeyse girmediği alan kalmamış ve buda beraberinde ciddi bir rekabeti getirmiştir. Türkiye'de olduğu gibi dünyada da özelleştirme konusu gündemi oluşturan konulardan biri olmuştur. Küreselleşme sonucu gelişmiş ve gelişmekte olan ekonomilerde baş döndürücü ölçekte yaşanan büyüme, karmaşıklaşan işlemler ve piyasa ilişkileri içinde oyunu kurallarına göre oynamamanın bedelinin çok pahalı olduğu anlaşılmıştır. Son yıllarda Dünyada ortaya çıkan muhasebe hileleri, mali raporlamanın güvenilirliğini sağlama konusunda iç kontrol sisteminin ve denetim sürecinin yeniden sorgulanmasını gündeme getirmiştir.

Ülkemizde de yaşanan ekonomik krizle birlikte karşılaşılan yolsuzlukların yanı sıra Avrupa Birliği uyum ve müzakere süreci; iç kontrol sistemi, iç denetim ve risk yönetimi ile ilgili uluslararası standartlarda yasal düzenlemelerin yapılmasına neden olmuştur (Delloitte, 2008). Türkiye de bu rüzgarlardan nasibini alırken kendi içinde ekonomisini etkileyen olaylara sahiptir. Tüm pazarlarda rekabetin artması ve hem ithalatın hem de ihracatın artması Türkiye ekonomisini etkileyen ilk başlıklar olmuştur. Sermaye piyasaları oluşmuş ve finansal kurumlarının çeşitlendiği görülmüştür. Bu ve benzeri sebeplerden dolayı tüm dünyada hem iyi hem de kötü yönde riskler artmaya başlamış ve buda risk yönetimi ihtiyacını doğurmuştur.

Ülkemizde ve piyasalarımızda karşılaşılan bazı negatif koşullar (Sezgin, 2008);

- Uzun vadeli yatırımlara yönelik kaynak yetersizliği,
- Mevzuat ve sektör standartlarının eksikliği,
- Şirketlerin taşıdıkları piyasa riskini bertaraf etmelerini sağlayacak enstrümanların yetersizliği,
- Nakit yönetimi sistemlerinin yerleşmemiş olması (Yüksek likidite riski),
- Daha yüksek olasılıklı beklenmedik olay risklerinin artması (event risk),
- Kaynak yaratılmasını sağlayacak piyasaların az gelişmiş olmasıdır.

Dünyada Kurumsal Risk Yönetimi

Risk yönetiminin iyi yönetimin vazgeçilmez bir unsuru olduğu anlayışı, başta gelişmiş ülkeler olmak üzere giderek tüm dünyada kabul görmektedir. Gelişmiş ülkelerin yüksek denetim kurumları da risk yönetimini başarılı bir yönetimin aslî unsuru olarak kabul etmekte ve uygulamaktadır.

İç denetim ve KRY'nin dünya ve ülkemizdeki gelişimine ilişkin kilometre taşlarını kısaca gözden geçirildiğinde; çağdaş iç denetim anlayışının oluşmasında önemli bir yapı taşı olarak nitelendirilen (IIA-inc) Uluslararası İç Denetçiler Enstitüsü'nün 1941 yılında New York'ta kurulması ile birlikte iç denetim dünyada profesyonel bir mesleki disiplin haline gelmiştir. İç denetçilerin KRY'e olan yaklaşımları ile KRY de bu disiplinde yerini almıştır.

Uluslararası mesleki örgütlenme sonucu uluslararası mesleki standartlar ve etik kurallar oluşturulmuş, mesleki sertifikasyon sınavları başlatılmıştır. ABD'de başlayan örgütlenme, 1982 yılında (ECIIA) Avrupa İç Denetim Enstitüleri Konfederasyonunun kurulması ile mesleğin Avrupa Birliğinde statüye kavuşmasını sağlamıştır. Enron ve WorldCom skandalları ile yaşanılan ciddi sıkıntılar sonucu kurumsal yönetim uygulamalarının güvence altına alınması için ABD'de yeni yasal düzenlemeler yapılmıştır. Sarbanes-Oxley Kanunu ile iç kontrol sistemi ve iç denetim ve KRY fonksiyonuna verilen önem daha da arttırılmıştır.

Standard & Poor's'un finansal olmayan şirketlerin derecelendirme çalışmalarında kurumsal risk yönetimi uygulamalarının da değerlendirme kapsamına alınacağını belirtmesi ile, özellikle uluslararası finans kaynaklarına ulaşmak isteyen ve bu nedenle bir kredi derecelendirme notu almak durumunda olan tüm şirketlerin etkin bir KRY modelini kurumlarında hayata geçirme zorunlulukları oluşmuştur. Bu durumun elbette ülkemize de önemli yansımaları olacaktır. Ülkemizde faaliyette bulunan başta büyük uluslarası şirketler olmak üzere, yurt dışındaki bankalardan kaynak sağlamak isteyen finansal kuruluş, holding ve diğer büyük şirketlerin de yakın zamanda KRY'ni hayata geçirmek zorunda kalacaklardır. Elbette bünyesinde KRY pratiği olan şirketler de vardır. Bu şirketlerin de başta kurumsal risk yönetimi kültürü olmak üzere, kurumsal risk yönetimi stratejilerini gözden geçirmek ve KRY modellerinin etkinliğini artırma zorunlulukları oluşmuştur.

Uğural (2008)'a göre ekonomilerin ve finansal piyasaların entegrasyonu, lokal düzenlemelerin yetersiz kalması, küresel düzenlemelerin eksikliği, bilgi edinme ve paylaşımdaki teknolojik kolaylık ve hız, sosyal sorumluluğa verilen önemin artması, geleceğe dair global ve yerel risk algısı ve güven endekslerindeki olumsuz etkileri ve uluslararası krizin bir müddet daha devam etme olasılığı, önümüzdeki dönemde riskleri şekillendirecek global faktörler ve eğilimlerdendir.

Türkiyede Kurumsal Risk Yönetimi

Ülkemizde Bankacılık Kanunu, SPK ve taslak halinde olan yeni Türk Ticaret Kanunu, Sarbanes-Oxley Kanununda yer alan esasları benimseyen bir yaklaşımla hazırlanmıştır. Dünya ile paralel düzenlemelerin yapıldığı ülkemizde çağdaş bir kurumsal yönetim için yasal çerçevenin belirlendiğini ve iç denetimde ulusal örgütlenmenin on yıllık kurumsal geçmişinin bulunduğu görülmektedir. Ancak iç denetim ve KRY'ni uygulamada iyileştirilmesi gerekli konular olduğu söylenebilir. Kurumsallaşmasını henüz tamamlayamamış aile işletmesi yapısı, kayıt dışı ekonomi, istikrarsız ekonomi, kurumsal yönetim ve iç denetimin uluslararası standartlarda ülkemizde uygulanmasının önündeki engelleri oluşturmaktadır (Uzun, 2008).

Risk yönetimi konusunda SAS Güney Avrupa Bölgesi Risk Uygulamaları Yöneticisi Renzo Traversini 2008'de Türkiye'ye gelmiş ve risk yönetimi hakkında konuşmuştur.

Türkiye'de bankaların risk yönetimi'ne büyük önem verdiklerini anlatan Traversini, Türkiye'nin sanılanın aksine kurumsal risk yönetimi konusunda birçok Avrupa ülkesinden ileride olduğunu söylemiştir.

Traversini Türkiye'de yasal zorunluluk olmamasına rağmen bankaların kurumsal risk yönetimi çözümleri'ne yöneldiklerini, bunun nedeninin de hem risklerin farkına varmak hem de performanslarını artırmak olduğunu belirtiyor. Traversini'ye göre Kurumsal Risk Yönetimi, bankalar için olmazsa olmaz bir konudur. Uluslararası rekabete hazırlanan bankalar için bunun önemi daha da artıyor. Renzo Traversini, "Sadece veriyi analiz etmek yeterli değil, veriye erişim de takip edilmeli" demiştir.

Ayrıca ülkemizde 1995 yılında kurulan (TİDE) Türkiye İç Denetim Enstitüsü ile ulusal mesleki örgütlenme gerçekleşmiştir. TİDE ile başlayan ulusal mesleki örgütlenme, Türkiye'de iç denetimin uluslararası standartlarda uygulanması, meslek mensuplarının uluslararası sertifikasyonu için imkan sağlamıştır.

Türkiye'deki reel sektörde risk yönetiminin yanlışlıkları ;

- Şirket çapında olmaması,
- Belirli risklere odaklanması,
- Entegre olmaması,
- Süreç sahibi inisiyatifinde olması,
- Strateji, hissedar değerlerine bağlı olmaması
- Denetim ile kapsanmaya çalışılması
- Yeterli bilgi birikimi olmaması,
- Gereksiz bürokrasi yaratması,
- Sigorta ile eşdeğer görülmesi,
- Üst düzey sahiplenmenin az olması,
- Bankacılıktaki risk yönetimi ile karıştırılması,

Tüm bu eksiklikler ile Türkiye'de risk yönetiminde hala geleneksel yaklaşımın ağırlık basdığı görülmektedir. Yeni bir yaklaşım olan kurumsal risk yönetimi anlayışının henüz ülkede çok yeni olduğu ortaya çıkmaktadır.

Risk Yönetimi ve Denetim Açısından Gelişmesi Gereken Yönler *(Sezgin, 2008)**;***

- Bağımsız denetim, bağımsız derecelendirme ve iç kontrol mekanizmalarının kurumsal yapı içine yerleştirilmesi,
- Riskleri belirleyen, ölçen, raporlayan altyapıların geliştirilmesi,
- Risklerin açık şekilde muhasebe uygulamaları ve raporlamalar içine yerleştirilmesi,

- Tüm bunları yerleştirecek teknik bilgiye (know-how) sahip kadroların yetiştirilmesi,
- Ürün/servis alım satımından oluşan risklerin daha iyi incelenmesi,
- İşlem yapılan tarafların risk ve risk yönetimi açısından da değerlendirilmesi,
- Operasyonel faaliyetlerde oluşan hataları kontrol edecek bağımsız mekanizmalar ve iç denetimden sorumlu birimlerin geliştirilmesi,
- Piyasa riski yönetimi
    - Piyasaların yeterince gelişmemiş olması,
    - Hedge enstrümanlarının yetersiz olması,

Önümüzdeki dönemde Reel Sektörde Yapılması Gerekenler; Reel sektör sadece kredi almak ve finansman sağlamak açısından değil, şirketi daha verimli yönetmek, büyütmek, geliştirmek ve uluslararası rekabet açısından aşağıdaki hususlara önem vermeli ve geliştirmelidir (Sezgin, 2008);

- Personel eğitimi ve kalitesi, risk yönetimi konusunda yetişmiş insan kaynağı,
- Muhasebe altyapısının uluslararası standartlara göre düzenlenmesi, her türlü işlemin muhasebe içine alınması, uluslararası kabul görmüş standartlarda, güvenilir mali tablolar üretilmesi, doğru ve zamanında raporlama ve şeffaf bilgi akışı sağlanması,
- Bağımsız denetim ve bağımsız derecelendirme kuruluşlarının değerlendirmesi,
- Finansal riskleri yönetecek, riskten korunma sağlayan ürünlerin öğrenilip daha etkin bir şekilde kullanılması (hedging imkanları),
- İç süreçlerin tüm iş akışlarını, risk ve kontrolleri içerecek şekilde oluşturulması,
- Teknolojik altyapı yatırımları ile veri tabanı, ölçümleme, raporlama sistemlerinin etkin hale getirilmesi,
- Satış ve pazarlama faaliyetleri, pazar konumu, rekabet avantajı, müşteriler ve tedarikçilerin her türlü risk açısından değerlendirilmesi.

Kurumsal risk yönetimi risk dolu ortamlarda yönetimlerin daha etkin çalışmasını sağlar; Türkiye gibi hareketli piyasalarda ise bu bir avantaj haline gelmektedir. Türkiye'nin uluslararası bir finans ve ekonomi oyuncusu olması isteniyorsa, risk

yönetimi konusundaki uluslararası standartların bir an önce kabul edilmesi ve uyarlanması gerekmektedir. Operasyonel risk yönetiminde ve risk temelli denetimde önemli uluslararası standartlar COSO'nun (kurumsal risk yönetimi çerçevesi ile Bank of International Settlements'in Basel II gerekleridir (Meriç, 2004).

SPK tarafından 27.7.2004 tarihinde Türkiye'de IMKB'de işlem gören şirketlere yönelik olarak yapılan kurumsal yönetim uygulama anketi sonuçlarına göre ;

- İMKB'de işlem gören ve anketi cevaplayan 249 şirketten %52'si, "Yönetim Kurulu tarafından oluşturulan risk yönetim ve iç denetim mekanizması"na sahip olduğunu belirtmiştir. Bu oran İMKB-30 şirketleri için %69'a çıkmaktadır.
- "Yönetim Kurulu tarafından Genel Kurula sunulmuş kamuyu bilgilendirme politikanız var mı?" sorusu %77 oranında "yok" şeklinde cevaplanmıştır. Bu oran İMKB-30 şirketleri için %69'dur.

9.2 KRY'e Olan Farkındalığı Ölçmek İçin Yapılan Araştırmalar

Bu bölümde, tez kapsamında yapılacak Türkiye'de reel sektördeki risk yönetim ve bağdaşık olarak iç denetim faaliyetlerinin varlığını sorgulamak amacı ile yapılan araştırmaya hazırlık aşaması olarak dünyada bu tarzdaki araştırmalar ve sonuçları anlatılmıştır.

1. Ernst&Young Kurum Bazında Risk Yönetimi Araştırması

Ernst&Young'ın, Ocak 2004'te Avustralya'da 52 şirket üzerinde yaptığı araştırmanın amaçları; mevcut risk yönetimi uygulamaları üzerinde karşılaştırmalı değerlendirmeler yapmak, öncü risk yönetimi uygulamalarının ne kadar yaygın kullanıldığını tespit etmek ve gelecekte ortaya çıkacak sonuçların izlenmesi için dayanak oluşturmaktır.

Araştırma sonuçlarına göre risk yönetimi uygulamalarını yapan şirketler "Sorun çıkaran risk"i anlamıştır. Bu anlayışın şirkete ve şirketin hissedarlarına değer katıcı olmasını sağlayacak etkili bir sistem geliştirmiştir. Risklerini görebilmek ve yönetmek için beraberinde doğru bir kültürü ve altyapıyı geliştirmiştir.

Bulgulara bakıldığında büyük bir çoğunluk (%84) organizasyon içerisinde riskleri yöneten etkili bir sürece halen sahip değildir. Yönetim kademesinde; şirketlerin sadece

%18'inin risk yönetim koordinatörü (CRO) vardır ve %36'sı ise risk yönetimi sorumluluğunu çeşitli departmanlara, fonksiyonel olarak dağıtmıştır.

Şirketlerin sadece %16'sı, kurumsal bazda tüm risklerini yönetecek resmi bir stratejiye sahiptir. Şirketlerin %19'unda, risk yönetimi politikaları ve prosedürleri için iletişim kanalları bulunurken, sadece %29'u, hedeflere yönelik risk bazlı planlar yapmaktadır. Şirketlerin sadece %19'u risk limitlerinin ve toleranslarının net bir tanımına sahiptir.

Finansal kurumlar ise, risk yönetimi için en kapsamlı yaklaşımları benimsemiş ve araştırmaya konu olan tüm finansal kurumlar, risk yönetimi fonksiyonuna sahiptirler. Finansal kurumların; % 84'ü kurum bazında riski yönetmektedir ve % 75'i de kurumsal risk sorumlusuna sahiptir. Finans kurumları dışındaki diğer sektörlerde ise, bankaların tam tersine risk yönetimi için kapsamlı bir yaklaşıma doğru daha yavaş ilerlenmektedir. Finans dışı kuruluşların; %83'ünün sorumlu bir risk uzmanı dahi yoktur. %73'ü ise risk yönetimi için yetersiz olduklarını ve gelişmeye ihtiyaç duyduklarını belirtmektedir.

Büyük şirketler risk yönetimi faaliyetlerini daha geniş bir yelpazede uygulamakta ve ciddi risk yönetimi yapılarına vakıflardır. Küçük şirketler formal olmayan teknikler kullanmakta ve küçük şirketlerin sadece %4'ü risk yönetimini uygun politikalar ve süreçlerle düzenlemiştir. 4 milyar USD'den az cirosu olan küçük şirketlerin sadece %17'si kendi iş fonksiyonlarına risk yönetimini entegre etmiştir.

Denetleme komiteleri ve yönetim kurulları risk yönetiminde giderek daha aktif olmaya başlamıştır. Denetim komitelerinin (ya da benzerlerinin) %86'sı kurum bazındaki risk hakkında düzenli olarak şirket yönetiminden güncel bilgi almaktadır. Denetim komitelerinin %74'ü risk yönetimi süreçlerini incelemektedir. Araştırmaya katılan şirketlerin yarısı, kendi denetim komitelerinin faaliyet kapsamını geliştirmeleri gerektiğini kabul etmektedir.

2. SAS - Chartis Research, "Kurumsal Risk Yönetimi" konulu araştırma'da Chartis research isimli araştırma şirketi ve iş zekası alanında dünya lideri olan SAS Institute'un 410 finansal şirket yetkilisi ile yaptıkları görüşme sonucunda kurumsal risk yönetimi konulu araştırma sonuçları Isveç Stockholm de SAS forum 2007'de açıklanmıştır.

Finans şirketi yetkililerine göre KRY sistemlerini tetikleyen sebepler performans yönetimi ve yasal düzenlemelerdir. Ayrıca KRY sistemi kullanan finansal şirketler

performans yönetiminde iyileşme kaydederken sermaye yeterliliği ve kredi kayıplarında düşüşler sağlamışlardır.

SAS tarafından gerçekleştirilen araştırmaya katılan 410 yöneticiden %60'ı KRY programının 24 ay içinde sermaye karşılık ayırma zorunluluğunu aşağıya çekmelerini sağlayacağını ve sermaye karşılığı oranlarında %8 düşüş yaratacağını vurgulamışlardır. Finans dünyasına göre, pazarın kendi risk faktörleri ve finans suçları öncelikler olarak ortaya çıkmıştır. Pazar risklerine odaklanmanın temeli de ölçeklenebilirlik ve hızdan yoksun geleneksel sistemlerinin değiştirilme ihtiyacından kaynaklanmaktadır. Araştırma sonuçlarına göre pek çok finans şirketi KRY'nin kurumlar için büyük faydalar sağlamasını beklerken yüzde 26'sı kurulum için zaman çizelgesi hazırlamış ve iyi formüle edilmiş bir stratejiye sahiptir. Buna rağmen finans şirketlerinin yüzde 25'inde KRY ile ilgili hiçbir strateji belirlenmemiş durumdadır.

Araştırmaya katılan yöneticilere göre başarılı bir KRY kurulumuna gerekli olan veri kalitesi ve veri yönetimidir. Riskleri yönetmek için kullanılan silo tabanlı yaklaşımlar, entegre ve konsolide edilmiş risk yönetimi sistem ve süreçlerinin sağladığı performans ve maliyet düşüşünü sağlayamamaktadır. Ancak değişik risk yönetimi sistemlerinin tek bir teknoloji ortamında entegre edilmesi tüm riskleri görmek için avantaj sağlamaktadır.

3. **Tillinghast-Towers Perrin Survey (2006), "Enterprise Risk, Management: Trends and Emerging Practices"**adlı çalışmada farklı sektörlerden 130 şirkete bir anket uygulanmıştır. Araştırma kapsamında hangi tip organizasyonların KRY'i uyguladıkları, ne zamandır ve ne ölçüde uyguladıkları gibi sorulara cevap aramışlardır.

Hedef kitlenin %27'si finansal servisler, %20'si enerji ve madencilik, %14'ü üretim, %9'u kamu ve %9'u da telekomunikasyon/IT sektörlerindendir . Bu organizasyonların %58'i geliri 1 milyar dolardan fazla, %66'sı ise varlıkları 1 milyar dolardan fazla büyüklükte ve %43'ü de çok uluslu veya global şirketlerdir.

Araştırmaya katılanların %49'u kısmi veya tam KRY programlarına sahip olduklarını, sahip olanların %75'i de iki yıl veya daha az bir zamandır KRY programı olduğunu söylemiştir. Geri kalan diğer kurumların neredeyse hepsi KRY'i ya araştırmakta yada uygulamayı planlamaktadır. Cevaplayıcılar, kurumsal yönetişim reformları ve politikaları KRY'nin kabulünde %38 etkili bulmaktadır. Firmaların %80'i aşkını

finansal ve operasyonel riskleri iç denetim planında dikkate alırken, yarısından azı stratejik riskleri bu planda önemsemektedirler.

Kullanılan risk yönetim teknikleri sorulduğunda; firmaların %50'sinin risk haritaları, %44'ünün risk değerlendirme workshopları kullandığı ortaya çıkmış, aynı zamanda yanlızca %28'nin şeklen finansal modelleme yaptığı, %20'sinin senaryo planlama ve %11'ninde olasılıklı simülasyon tekniklerini kullandığı ortaya çıkmıştır.

Çalışmadan çıkarılan bir diğer sonuç ise, firmaların KRY'in tam değerinin farkında olmadıklarıdır, çünkü çoğu bir yönetim aracı olarak görmektedir. Örneğin firmaların üçte birinden azı risk yönetimine sermaye ayırmakta, ve sermaye gerekliliklerini belirlemektedir. Organizasyonların %25'inden azı kısmı veya tam KRY programlarını risk yönetim stratejileri için teşvik ve karşılık olarak bağlamıştır.

Kurumlar organizasyonlarında risk yönetimini üstelenecek roller ararlar, cevaplayıcılar kurumlarında risk yönetiminden sorumlu tek bir idareci olduğu, bunun da genelde CEO (%45) olduğu sonucuna ulaşmıştır. Araştırmadaki KRY uygulayan firmaların %26'sında bu görevi denetimden sorumlu baş yöneticisi (CAO), %24'inde ise CRO (Risk Yönetim Direktörü) veya CFO üstlenmektedir. Genel olarak yöneticilerin kökeni risk yönetiminden değil de finans veya denetimden gelmektedir. Araştırmadaki bulgulara göre; yöneticilerin %21'i iç denetimden %18'i finanstan ve yalnızca %11'i risk yönetiminden gelmektedir. İç denetimin risk yönetiminde önemli bir rol oynadığı araştırmada da vurgulanmış ve araştırmaya katılanların %32'si iç denetimin KRY'e yön verdiğini söylemişlerdir. Birçok yönetici de "KRY'nin ön ucunu stratejik planlama ile arka ucunu ise denetim fonksiyonu ile bağlanması gerektiğini" söylemiştir.

4. Beasley ve diğerlerinin (2005)'de yayınladığı **Enterprise risk management: An empirical analysis of factors associated with the extent of implementation** adlı bilimsel araştırma Mart 2004'de IIA'nın üyesi olan 1770 firmaya IIA'nın elektronik daveti ile yapılmış ve bütün datalar toplandığında 175 cevabın olduğu hesaplanmıştır. Bu da geri dönüşün %10.3 olduğunu gösterir. Bu oran diğer iç denetim araştırmalarına (%30 geri dönüş oranına sahip) göre düşük olsa da diğer araştırma sonuçları ile uyumlu bulunmuştur. 52 firmanın cevabı da yarım yada uygun olmadığından regresyon analizine katılmamıştır. 123 organizasyondan ibaret sonuç model çok değişkenlidir.

Colquitt ve diğerleri (1999)'un bulgularına göre büyük ölçekli firmalar entegre risk yönetimine uyum sağlamakta küçük firmalardan daha şanslı ve etkili bir KRY kurulumu ve teknikleri için daha büyük kaynaklara ihtiyaç olması ve büyük firmaların bu kaynakları sağlayabilmesi bunun etkenlerinden bulunmuştur.

Bu araştırmada da bazı endüstrilerin (bankalar, eğitim ve sigorta kurumları) KRY'i kabul edip yerleştirmede diğerlerinden daha şanslı oldukları tespit edilmiştir. Bankalar risk yönetimine gelen minimum sermaye gerekliliğini azaltma yolu olan global düzenlemeler (Basel II, 2004 vs.) ile bu konuda lider, eğitim kurumları KRY'i adapte etmek için teşvik eden önemli düzenlemelere sahip ve sigorta şirketleri daha iyi risk esaslı karar verme ve sermaye dağılımı aracılı sermayedar değeri geliştiren ve yaratan esas araç olarak kurumsal risk yönetimini tanır hale gelmeye başlamışlardır.

Araştırma sonuçlarına göre; Amerikanın daha güçlü bir kurumsal yönetim yapılanması olmasına rağmen KRY'e adaptasyonda Australya, Yeni Zelanda, Güney Afrika, ve İngiltere ülkelerinden daha geride kalmışlardır. Araştırmaya göre Asya-Pasifik bölgesi CEO'larının % 46'sı ve ABD CEO'larının ancak % 28'i KRY'e öncelik vermektedir. Modelin %50'si (62 şirket) KRY'i kısmen veya tamamen uygulamakta, %35'i ise KRY'i yerleştirme konusunda hiçbir plan yapmamış veya uygulama kararı almamıştır. Ayrıca kurumların %31'inde CRO görevli ve kurumlardan %88'i büyük bir denetleme firmaları tarafından denetlenmektedir. Sonuçlardan büyük ölçekli ve dört büyük firma tarafından denetlenen kurumların daha kolay KRY'i kabul ettiği ortaya çıkmıştır.

Sonuçlar gösteriyorki; KRY'de üst yönetim ve yönetim kurulu liderliği KRY adaptasyonunu genişleten kritik etkenlerdendir. Büyüklük, sektör, denetim tipi, ülkenin yeri gibi diğer organizasyonel faktörler de etkilemektedir.

5. PricewaterhouseCoopers (PwC) tarafından Ocak 2004'te gerçekleştirilen, CEO'ların özellikle risk ve risk yönetimi hakkındaki görüşlerine yer veren 7. Yıl CEO Anketi'nin sonuçlarına göre: CEO'ların üçte ikisinden fazlası riskin belirlendiği, ölçüldüğü ve yönetildiği süreçlerin mevcut olduğunu belirtmiştir. Buna karşın, araştırmaya katılan CEO'ların sadece %23'ü ortak bir terminolojiye ve risk yönetimi için bir takım standartlara sahip olduklarını belirtmiş ve sadece %26'sı tüm

organizasyon çapında bir risk yönetimi için gerekli bilgilere ve verilere sahip olduklarından emin olduklarını belirtmişlerdir.

Organizasyonlarının içinde KRY'nin ölçümünün ve entegrasyonunun anlaşılması konusunda ise CEO'ların %26'sından azı bu konuda yeterli oldukları yanıtını vermişlerdir. CEO'ların sadece üçte biri mevzuata uygunluk aktivitelerinin riskleri azalttığını düşünerek bundan tatmin olmakta ve sadece üçte biri bu aktivitelerden kaynaklanan maliyetleri tam anlamıyla takip edebilmektedir.

Ortalama olarak CEO'ların %38'i halihazırda etkili ve verimli KRY'ye sahip olduklarını düşünmektedir. Eğer KRY CEO'nun, yönetim kurulunun ve tüm organizasyonun önceliği olduğu düşünülüyorsa, organizasyonun tam anlamıyla baştanbaşa entegre edilmiş sistemlere sahip olması gereklidir.

Anket sonuçlarından görüldüğü üzere, KRY'nin faydaları ve gerekliliği giderek en üst seviyede tanınmakta ve bu konudaki bilinç ve anlaşılırlık gitgide yayılmaktadır. KRY'ye olan ihtiyacın sadece düzenleyicilerden kaynaklanmaması ve şirketlerin bu olguyu bir yönetim aracı olarak tanımaları da ayrıca önemlidir.

6. Prof. Dr. Yunus Kishalı ve Arş. Gör. Davut Pehlivanlının 2006'da yayınlanan **Risk Odaklı İç Denetim ve İMKB Uygulaması** adlı makalesinde yayınlanan araştırma, 100 şirketin denetim koordinatörü, denetim yönetmeni, mali koordinatör pozisyonunda yer alan isimlerine eğer bu pozisyonlar yer almıyorsa genel müdür pozisyonundaki yetkililerine gönderilen anketler ile gerçekleştirilmiştir. Cevaplanma oranı 0,36 olan araştırma, firma genel bilgileri, iç denetim bilgileri ve risk değerlendirme ve risk odaklı iç denetim üç kısım olmak üzere toplamda yirmi sorudan oluşmuş ve sorular, literatür çalışması ve denetim meslek dergilerinden hareketle hazırlanmıştır.

Cevaplayıcıların % 27,8'i finans/bankacılık, % 63,9'u üretim/perakende, geri kalan %8,3'ü de hizmet sektöründe faaliyet göstermektedir. Sonuçlara göre şirketlerin %16,7'sinin iç denetim birimine sahip olmadığı, % 41,7'sinin iç denetim biriminin 1-2 kişiden oluştuğu, % 13,9'unun 4-6 kişi, % 5,6'sının 7-9 kişi, % 2,8'nin 10-12 kişiden oluştuğu son olarak da % 19,4'ünde ise 17 ve üstü (tümü finansal kuruluşlar) iç denetim elemanı bulunduğu belirlenmiştir.

2000 yılında Nahit Akarkarasu tarafından yapılan (Halka Açık Şirketlerde İç Denetim ve Denetim Kurullarının Etkinleştirilmesi için Öneriler) çalışmada İMKB 100'de yer alan şirketlerin % 61'inin iç denetim birimine sahip olmadığı sonucuna ulaşılmıştır. Aynı araştırmaya göre iç denetim birimine sahip şirketlerin % 16'sının da yasal zorunluluklar sonucunda bu birimi oluşturdukları anlaşılmıştır. Buna göre geçen süre zarfında iç denetim birimine sahip işletme oranında önemli bir artış meydana gelmiştir.

Çalışmada, iç denetimin organizasyon içindeki yerinin belirlenmesi açısından sorulan soruya verilen cevaplardan % 19,4'ünün denetim komitesine, yine % 19,4'ünün yönetim kurulu başkanına, % 13,9'luk oranlarla yönetim kurulu üyesi veya genel müdür/yardımcılarına, % 8,3'ünün de CEO'ya bağlı oldukları sonucuna ulaşılmıştır. Holdinge bağlı faaliyette bulunan işletmelerin % 30,6'sında ana şirkette, % 5,6'sının bütün holding şirketlerinde, % 44,4'ünde ise bir veya daha fazlasında denetim departmanı olduğu sonucuna ulaşılmıştır. İşletmelerin % 56,3'ünün yıllık iç denetim planlarını finansal tabloların denetimine % 10'unun altında zaman ve kaynak ayırdıkları; % 65,6'sının faaliyet denetimine en fazla % 30 zaman ve kaynak ayırdıkları; bilgi teknolojilerinin denetimiyle % 40,6'sının hiç ilgilenmediği son olarak da risk değerlemeyle % 28,1'inin ilgilenmediği ve risk değerlemeye % 62,5'inin de kaynak ve zamanlarının en fazla % 10'unu ayırdıkları görülmüştür.

Risklerin tanımlanması, sınıflandırılması ve ölçülmesi aşamalarından oluşan risk değerleme faaliyetlerini cevaplayıcıların % 66,7'sinin kullandığı geri kalan %33,3'ünün ise kullanmadığı görülmüştür. Finans sektörü için yasal zorunluluk olduğu nedeniyle bu oran % 100 iken, üretim/perakende sektöründe faaliyet gösteren şirketlerden %52,3'ünün risk değerlendirme aşamalarını kullandığı sonucuna ulaşılmıştır.

Risk değerlendirme aşamalarını kullanan cevaplayıcıların % 50'si iç denetim biriminin risk yönetim birimi ile ortak çalıştığını, % 27,3'ü risk değerlendirme faaliyetinin dış danışmanlar desteğiyle iç denetim birimi tarafından yürütüldüğünü, % 22,7'si ise iç denetçilerin rolü olmadıklarını ifade etmişlerdir. Risk değerlendirme aşamalarını kullanan cevaplayıcılardan, % 87,5'inin denetim planını risk odaklı yaklaşım çerçevesinde hazırladıkları kalan % 12,5'inin de üst yönetimin istekleri doğrultusunda denetim planını hazırladıkları görülmüştür.

10. TÜRKİYE ENERJİ SEKTÖRÜNE YÖNELİK KURUMSAL RİSK YÖNETİM FARKINDALIĞI ARAŞTIRMASI

10.1 Araştırmanın Amacının, Hedef Kitlesinin, Yönteminin Belirlenmesi ve Soru Setinin Hazırlanması

Kurumsal risk yönetimi üzerine yaptığımız teorik araştırmaya dayanarak Türkiye'de çok da sorgulanmayan KRY uygulamalarını tespit etmeyle çalışmaya başlanmıştır. Araştırmada öncelikli amaç Türkiye'deki risk yönetim uygulamalarının yapısını belirlemek ve bu yapılar içinde kurumsal risk yönetiminin yerini ve uygulanışını çözümlemektir. Yani kısa deyimiyle Türkiye kurumsal risk yönetimi profilini çıkarmak ana amaçtır. Bu amaca ek olarak uygulamada KRY yapılarının iç denetim ile ilişkisini de gözler önüne sermek ikincil amaç olmuştur. Amaç belirlendikten sonra araştırmaya hedef kitle belirlemek ile devam edilmiştir. Literatürden çıkardığımız, küçük çaplı şirketlerde kurumsal risk yönetiminin başarılı olamayacağı ve güçlerinin bu yapıyı yerleştirmeye yetemeyeceği öngörüsü ile büyük çaplı firmalara yönelik bir araştırma yapmanın daha mantıklı sonuçlar vereceğine karar verilmiştir. İlk olarak, İstanbul Sanayi Odası (İSO)'nın büyüklük bakımından sıraladığı ilk 500 şirket ölçüt alınmıştır.

İlk önce bu 500 şirket içinden sektör belirlemek amacıyla şirketlerin üretim bilgileri de alınarak sektörel olarak gruplandırılmıştır. Şirketlerden elemeler yapılmış ve en son tekstil, gıda, enerji ve ilaç/sağlık olarak dört sektöre gelindiğinde konu ile bilgili ve tecrübeli kişiler ile fikir istişaresi yapılmıştır. İlaç ile enerji sektörünün daha profesyonel kurumlar olduğu, anlayış kabiliyetleri, konuya farkındalıkları ve araştırmaya destek verebilme ihtimallerinin daha yüksek olması ile tekstil ve gıda sektörleri elenmiştir. S&P'nin finans dışı sektöre getirdiği KRY kriterini uygulamayı da ilk olarak en aktif sektör olan enerji sektöründe uygulamaya başlaması ve ilaç sektörü sorgulandığında olumlu cevapların gelmeyişi hedef kitelemizin yapısını sonlandırırken yardımcı olmuştur. Ve ilk olarak hedef kitle İSO'nun açıkladığı ilk 500 şirket içindeki

petrol ve elektrik firmalarını içeren enerji firmaları olarak belirlenmiştir. Ancak İSO 500'de olan 31 enerji firmasından literatürdeki araştırmaları baz alarak geri dönüş oranının %25 ları aşmayacağı verisi ile ancak 7-8 firmadan cevap alınabilceği öngörülmüştür. Bu nedenle hedef kitleyi genişletme ihtiyacı duyulmuş ve büyüklük ölçütünün çok dışına çıkmamak temel kriter olmuştur. Ve Türkiye enerji sektöründe İSO 500 büyük ölçütüne yakın faaliyet gösteren 14 firma daha bulunmuş ve hedef kitleye eklenmiştir. Böylelikle enerji sektöründe faaliyet gösteren büyük ölçekli 45 firmayla iletişime geçilmiştir.

İSO'dan talep edilen erişim bilgileri CDsi ve firmaların internet sitesinden alınan numaralar vasıtası ile kurumlarla telefon bağlantısına geçilmiştir. Önce telefonla firmalardaki gerekli kişilere ulaşılmaya çalışılmış, ancak bir çoğunun "e-posta ile talepte bulununuz" isteği üzerine ve telefonla ulaşılamayanlara talebimiz e-posta ile yazılı olarak bildirilmiştir. Teknik olarak öncelikle "face to face interview" denilen birebir görüşme tekniği belirlenmiştir lakin firmaların istekleri doğrultusunda hazırlanan soru seti anket tarzına dönüştürülmüştür. Bu tarz ile sonuçları analiz etmek ve araştırma sınırlarını belirlemek daha kolay hale gelmiştir. Firmalardan gelen cevaplara göre, birebir görüşme, telefonla görüşme ve elektronik posta ile haberleşme olmak üzere üç türlü teknik kullanılmıştır.

Soru setindeki sorular hazırlanırken literatür araştırması, dünyadaki benzer araştırmalar, düzenleyici yasal mevzuatlar, kurumsal risk yönetimi ve iç denetim gereklilikleri referans alınmıştır. Soru seti risk yöneticisinin ve şirketin büyüklük profilini çizerek başlamaktadır. Risk yönetimine ilişkin genel sorular ve iç denetim ile ilgili soruları kapsayarak devam eden set, uygulanan yönetim yaklaşımı ile kuruma getirilen fayda ve zorlukları sorgulayarak son bulmaktadır. Anket Ek-A.1'de yer almaktadır.

Firmalara ulaşmak ve firmalardan bilgileri toplamak yaklaşık 40 gün sürmüştür. 19 Kasım 2008 tarihinde firmalarla iletişime geçilmeye başlanmış 29 Aralık 2008 tarihinde ise en son geri dönüşü alarak araştırmanın bilgi toplama aşamasına son verilmiştir.

10.2 Alınan Geri Dönüşler

Telefon görüşmesiyle ile iletişime geçilen hedef kitledeki 45 firmanın 12'si ya konuyla ilgilenmemiş ve görüşme veya e-posta ile anket talebimize cevap vermemişlerdir. 29 firma ise "öncelikle soru setinizi gönderin" şeklinde talebimize geri dönmüşler ve istekleri doğrultusunda soru seti elektronik ortamda taraflarına ulaştırılmıştır. Ancak bir çoğu soru setimizi istedikten sonra hiçbir geri dönüşte bulunmamışlardır. Geriye kalan 4 firma ise görüşme talebimize olumlu cevap verip, üçü birebir görüşme olan birisi telefonda görüşme olan randevular vermişlerdir. Diğer 29 firma içinden dördü de sorularımızın hepsine elektronik ortamda cevap vermiştir. Kalan 25 firma arasından 10 firmanın telefondaki görüşmelerden çıkarılan sonuçlarına göre, üç firma Türkiye'nin en büyük holdinglerinden birine bağlı olup kurumsal risk yönetimini holding çapında uygulamaktadır. Ayrıca 10 şirkette de ya holdinge bağlı yada ana şirket faaliyeti olarak risk yönetim veya iç denetim birimi oldukları bilgileri alınmış, birinden ise planlanan projeler arasında kurumsal risk yönetimini kuruma yerleştirmek olduğu bilgisi alınmış, ama tüm sorularımıza cevap alınamamıştır. 10 şirketten biri holdinge bağlı olarak yürütülen, birisi ana şirket faaliyetlerinden olan ve birisi de çokuluslu bir firma olup, ABD'deki merkezlerine bağlı olan Türkiye'deki firmalarında da bir iç denetim yapılanmasının var olduğunu söylemiştir. On firmadan 7'si ise risk yönetimi ve iç denetim adı altında bir yapılanma olup, risk odaklı denetim anlayışı veya kurumsal risk yönetimi anlayışı ile risk yönetimi uygulamalarını yaptıklarını belirtmişlerdir.

10.3 Firmalardan Alınan Bilgiler

Şirketlerden alınan cevaplara göre; yukarda belirttiğimiz sorularımızın tamamını cevaplamayan ama kısa bilgi veren 10 firmadan yedi firmaya ilaveten soruları cevaplayan altı firma daha kurumsal risk yönetim uygulamaları olduğunu belirtmiştir. Diğer ikisi ise risk yönetim uygulamasının olmadığını ancak biri risk yönetimini planlayıp araştırma aşamasında olduğunu söylemiştir.

Elektronik ortamda soruları cevaplayan, 13.000 personel ile 25 yılı aşkındır elektrik üretimi yapan ve kamusal alanda faaliyet gösteren firma ise risk yönetiminin plan dahilinde bile olmadığını ancak kamu kuruluşu olması nedeniyle yasalarda ve

yönetmeliklerde belirtilen mevzuatlar çerçevesinde kurum bünyesinde yer alan Teftiş Kurulu Başkanlığınca uygunluk denetimi ve faaliyet denetimi görevleri ile denetlemelerin yapıldığını bildirmişlerdir. Bu birim gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetlemekte ve İç denetçi, işletmenin varlıklarının ve kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını değerlendirmektedir. İç denetim, iç denetim raporuna uygun olarak tamamlanmasını denetleyerek kendi etkinliğini de ölçmektedir. Ayrıca zorunluluk gereği bir dış denetçi ile çalışmaktadırlar.

Kurumsal risk yönetimini araştırma ve planlama aşamasındaki Türkiye enerji sektörünün en önemli oyuncularından biri olan firma ise 43 yıldır faaliyet göstermekte ve 3 bin 700 kişi istihdam etmektedir. Sorularımızı elektronik ortamda, yanıtlayan kurum çapında risk yönetiminden sorumlu uzman yardımcısı işletme eğitimi almış ve kurumda da üç yıldır görev yapmaktadır.

Bu büyüklükteki firma kurum çapında uygulamaya geçerken risk haritaları oluşturarak riskleri belirlemeyi tamamlamıştır. Belirlediği riskleri kurum çapında değerlendirme ve kontrol aktiviteleri uygulamayı, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermeyi, risk finanslama çözümlerini belirleyip uygulamayı yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmayı kuruma yerleştirmeye devam etmektedir. Risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri karşılamak, şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulamak, bir risk yönetim raporlaması ve bilgi sistemi kurmak, kurum çapında risklerin takip edilmesi, şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmak faaliyetleri ise şirketin planları arasındadır. Bu faaliyetlerin planlama veya yerleştirmeye devam dahilinde dahi olması şirketin kurumsal risk yönetim dönüşüm sürecinin başladığını göstermektedir. Şirket genelinde risk yönetimi konusunda bilgi eksikliği kurumsal risk yönetim sürecini entegre ederken kaşılaştıkları en büyük zorluk olmaktadır.

Firma hangi risk grubuna daha çok odaklanmaktasınız sorusuna karşılık olarak odaklandıkları risk gruplarını öncelik sırasına göre stratejik, finansal, çevre, ve

operasyonel olarak belirtmiştir. Bunun yanında iç denetim konusunda hiçbir faaliyet ve yönetmeliğin de bulunmadığını söylemişlerdir.

Elektronik ortamda sorularımıza cevap veren diğer şirket ise 77 yıldır enerji sektöründe özellikle petrol ile faaliyet göstermekte ve 500'ü aşkın çalışanı bulunmaktadır. Stratejik birim altında kurumsal risk yönetim uygulaması var olan şirketin uygulamayla ilgili bilgiler, mühendislik eğitimi almış, kurumda risk yönetiminden 5 yıldır sorumlu ve CFO'ya bağlı Hissedarlar Servisi Müdürü'nden alınmıştır.

Daha etkin iç denetim ve kontrol ihtiyacı ve artan kriz frekansına uygun bir kriz yönetimi ile krizlerin atlatılması amacı ile başlanılan, ana şirket faaliyeti olarak üç yıldan fazla zamandır yürütülen risk yönetim uygulaması tamamen yerleşik durumdadır. İç kontrol ve risk yönetimi fonksiyonlarını yürütmekte olan kişi sayısı sorulduğunda 3–5 şıkkını tercih eden firma risk yönetimi ve iç denetim çalışanlarının bilgi ve becerilerini artırmaya yönelik eğitimler yapmaktadır. Riskler ve risklere karşı yapılan uygulamalar üst yönetim ve paydaşlara raporlanmaktadır.

Soru seti kapsamında, risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, risk finanslama çözümlerini belirlemek ve uygulamak, kurum çapında riskleri karşılamak, şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulamak faaliyetlerini kurumlarında tamamen yerleşik hale getiren firma, yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak faaliyetini yerleştirmeye devam etmektedir. Planlanan faaliyetler ise bir risk yönetim raporlaması ve bilgi sistemi kurmak, kurum çapında risklerin kontrol aktiviteleri, kurum çapında risklerin takip edilmesi ve şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmaktır.

Risklerin belirlenmesi ve ölçülmesi için temel performans ve temel risk göstergeleri kullanan firma uygulamaya geçerken bir risk haritası çıkarmış daha sonra haritalandırma yapmamıştır. Kurumsal risk yönetimi kapsamında "Risk Management Standard"ını uygulayan firma odaklanma sırasına göre finansal, operasyonel, stratejik, ve çevre risklerine karşı uygulamalar yapmaktadır. Hedefledikleri yapıdan sapmadan kurumsal risk yönetimini firmalarına bir danışmanlık hizmeti alarak yerleştiren risk

yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını ayda bir gözden geçirmektedir.

İç denetim işlevinin sürdürülmesi ile görevli yönetim kurulu üyesi aynı zamanda risk yönetiminden de sorumlu olmamakta, bu görevden üst düzey risk komitesi sorumlu olmaktadır. İç denetim yönetimi gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğu ile işletmenin varlık ve kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını değerlendirmektedir. İç denetim bir dış denetçi tarafından denetlenmenin yanı sıra yaptığı iç denetimlerin iç denetim raporuna uygun olarak tamamlanıp tamamlanmadığını denetleyerek de kendi etkinliğini ölçmektedir. İç denetim biriminin denetim işlevlerinden en önemlisi finansal denetimdir. Risk yönetiminin denetimini de yapan birim bu görevi de ikinci önemli görev olarak görmektedir. Ardından önem sırasıyla uygunluk denetimi, güvence, danışmanlık, faaliyet denetimi, ve iş/süreç geliştirme görevlerini de yürütmektedir.

Firma yerleştirdiği kurumsal risk yönetimi uygulaması ile stratejik hedeflere ulaşılma, yeni pazarlara girme, karlılığın artması, rekabet edebilme, düzgün kurumsal yönetim prosedürleri oluşturma, paydaş/hissedarlara gerekli bilgileri aktarma, performans izleme konularında yararlar sağlamıştır. Bu yararları firmaya sağlarken, kurumsallaşma eksikliği, devlet politikalarındaki değişiklikler ve ekonomik koşullar firmanın karşılaştığı engeller olmuştur.

Elektonik ortamda sorularımızı cevaplayan son şirket ise enerji sektöründe faaliyet gösteren Türkiye'nin hatrı sayılır bir grup şirketi olup 500'ün üzerinde çalışanıyla 25+ yıldır faaliyet göstermektedir. Kurumsal risk yönetimini risk yönetim birimi altında yürüten şirketin uygulamayla ilgili bilgilerini lisanüstü seviyede makine mühendisliği eğitimi almış, 5 yılı aşkındır risk yönetiminde deneyimli olan, bu şirkette ise 2 yıldır görev yapan Risk Yönetim Bölüm Başkan'ından almış bulunmaktayız.

Performans eksikliği ile operasyonların verimliliğinin ve sürekliliğinin sağlanması, kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması, finansal risklere karşı korunma ve finansal değişikliklerden faydalanma ihtiyacı ile başlamış olan uygulama iki yıldır grup şirketine tamamen yerleşik duruma gelmiştir.

Risk yönetimi fonksiyonlarını 3–5, iç denetim fonksiyonlarını ise 11+ çalışanla yürüten firmadan bu birimlerde çalışanların bilgi ve becerilerini artırmaya yönelik yapılan eğitimler vardır. Risk raporlama sistemi ile üst yönetim, yönetim kurulu, paydaşlar ve ilgili şirketler ve departmanlara bilgi veren uygulamanın bir risk yönetim tüzüğü (risk yönetiminin amaçlarını ve taahhütlerini belirleyen resmi doküman) vardır ve bu tüzük şirketin tüm çalışanlarına bildirilmiştir.

Risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, risk finanslama çözümlerini belirlemek ve uygulamak, kurum çapında riskleri karşılamak, şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulama, yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak, bir risk yönetim raporlaması ve bilgi sistemi kurmak, kurum çapında risklerin kontrol aktiviteleri, kurum çapında risklerin takip edilmesi, şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmak faaliyetlerinin hepsini şirket tamamiyle yerleştirmiş durumdadır.

Temel performans göstergeleri, temel risk göstergeleri, iç değerlendirme araçları ve ayda bir yapılan risk haritaları (belirleme, tanımlama ve önceliklendirme) ile riskler belirlenmekte ve VaR, Monte Carlo, vb sayısal yöntemler kullanarak ölçümleme işlemi yapılmaktadır. Finansal, stratejik, operasyonel risk gruplarına aynı önem derecesinde odaklanan yönetim, KRY konusunda şirket genelinde Coso, Australian Standard (AS/NZS 4360) ve Risk Management Standard'larını uygulamaktadır.

Risk Yönetimi konusunda hiçbir harici danışmanlık hizmeti almamakla birlikte hedefledikleri risk yönetimi ile şuan uygulamakta oldukları risk yönetim arasında fark olmadığını belirten risk yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını üç ayda bir gözden geçirmektedir.

İç denetim işlevinin sürdürülmesi ile görevli yönetim kurulu üyesi aynı zamanda risk yönetiminden de sorumlu değildir. Üst düzey risk komitesi tamamen iç denetimden alakasızdır. Risk yöntiminden bağımsız çalışan iç denetim, gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetlemekle birlikte işletmenin varlıklarının ve kaynaklarının etkin bir şekilde kullanılıp

kullanılmadığını değerlendirmektedir. Her firma gibi bir dış denetçi tarafından denetlenen firmada iç denetim finansal denetim başta olmak üzere uygunluk ve faaliyet denetimi yapmakta ancak kendi etkinliğini ölçmemektedir.

Risk yönetimi firmanın değer yaratacak riskleri almasını, stratejik hedeflere ulaşmasını yasal ve idari düzenlemeler'e uymasını, düzgün kurumsal yönetim prosedürleri oluşturmasını sağlamanın yanında paydaş/hissedarlara gerekli bilgileri aktarmayı, performansı izlemeyi, karar mekanizmalarının ve iletişim ağlarını netleştirmeyi de kolaylaştırmıştır. Ayrıca risk yönetimine işletme içinde karşı olanların varlığı ile şirket, KRY uygulamayı yerleştirmekte zorlanmıştır.

Birebir görüşme tekniği uygulanarak sorularımıza cevap aldığımız üç şirketin ikisi holdinge bağlı şirketlerdir, diğeri ise ABD'deki merkeze bağlı ama Türkiye'de de faaliyet gösterip örgütlenen bir firmadır. Bu üç firmada kurumsal risk yönetim uygulaması ile alakalı faaliyetler görülmektedir.

İlk firma, enerji sektöründe faaliyet göstermenin yanı sıra birçok sektörde ağırlık olarak daha fazla yer almaktadır. Türkiye'deki belli başlı holdinglerden birisi olup 17.000 çalışanı ile 73 yıldır faaliyet göstermektedir. Enerji sektöründeki faaliyetleri ise yaklaşık 4 yıl önce başlamıştır. Daha otomasyonel faaliyetlerle enerji üretimi yapan firmanın enerji kolundaki istihdam sayısı 30 kişi civarındadır. Ama holdingin tüm yönetimsel faaliyetlerinde yerini almıştır.

Risk yönetim ve iç denetim başkanlığı altında risk yönetimi ve iç denetim ayrı ayrı bölümler olarak faaliyet göstermektedir. Kurumsal risk yönetim faaliyeti lisansüstü seviyede işletme eğitimi alan, sekiz yıldır risk yönetiminde, sekiz aydır da bu şirkette yöneticilik yapan bir müdür ile yürütülmektedir. Hem iç denetim müdürü hemde risk yönetim müdürü ile yapılan toplantıdan aldığımız bilgiler ışığında kurumsal risk yönetim sürecinin organizasyonel olarak yerleştirildiği ancak araçlar olarak hala yerleştirilmeye devam edildiği söylenebilir.

Kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması, artan kriz frekansına uygun bir kriz yönetimi ile krizlerin atlatılması ve performans eksikliği ile operasyonların verimliliğinin ve sürekliliğinin sağlanması ihtiyacı ve en önemlisi de kurumsal

yönetimin gerekliliği olarak kurumsal risk yönetim uygulaması 2 yıl önce planlanmaya ve yerleştirilmeye başlamıştır. Risk yönetimi faaliyetlerini risk yönetimi ve iç denetim daire başkanlığına bağlı olarak yöneten bir müdürün yanı sıra risk yönetim organizasyona katılması planlan 4 pozisyonla daha devam ettirmektedir. İç denetimde ise bir müdürle birlikte 13 kişi faaliyet göstermektedir. Tüm bu çalışanların bilgi ve becerileri sürekli sağlanan eğitimlerle artırılmaktadır.

KRY uygulamasının başlamasından itibaren yönetim kuruluna yapılan devamlı bir raporlama sistemi mevcuttur. Uygulamaya başlamadan önce KRY'nin amaçlarını, proseslerini ve taahhütlerini içeren bir risk yönetim tüzüğü hazırlanmış ve tüm çalışanlara bildirilmiştir.

Risk yönetim prosesini ve/veya fonksiyonunu organize etmeyi tamamen bitirmiş olan yönetimin halen devam etmekte olduğu faaliyetler; kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, kurum çapında riskleri karşılamak, bir risk yönetim raporlaması ve bilgi sistemi kurmak, kurum çapında risklerin kontrol aktiviteleri, kurum çapında risklerin takip edilmesi, şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmaktır. Risk finanslama çözümlerini belirlemek ve uygulamak, şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulama ve yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak ise yapılması planlanan faaliyetlerdir.

Temel performans göstergeleri, temel risk göstergeleri, iç değerlendirme araçları, şimdiye kadar sadece bir kez yapılmış ancak yılda bir yapılması planlanan risk haritaları (belirleme, tanımlama ve önceliklendirme) ile riskler belirlenmektedir. VaR, Monte Carlo, vb sayısal yöntemler kullanarak ölçümleme işlemi de yerleştirilmesi devam eden uygulamalardandır. Operasyonel riskleri başta olmak üzere stratejik risklerine de yeterince önem veren firma çevre risklerine ve daha sonra da az öneme sahip şekilde finansal risklerine odaklanmaktadır.

Kendilerine COSO'nun çerçevesini klavuz alan firma hedeflediği doğrultuda KRY fonksiyonlarına devam etmektedir. Hiçbir harici danışmanlık hizmeti almasada Türkiye'de bu yönetimi benimseyen firmalardan görüşler aldıklarını belirtmişlerdir.

İç denetim işlevinin sürdürülmesi ile görevli yönetim kurulu üyesi aynı zamanda risk yönetiminden de sorumlu olup iç denetim ile ilgili üst düzey risk komitesinde yer alabilecek kişiler bulunmaktadır.

Gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetlemek, işletmenin varlıklarının ve kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını değerlendirmek faaliyetlerini de yerine getiren iç denetim öncelik olarak iş/süreç geliştirme başta olmak üzere uygunluk ve faaliyet denetimini de yapmaktadır. İç denetim birimi, risk yönetim birimi kurulmasıyla birlikte risk yönetim görevini devretmiş ama genel denetimlerde RY birimini de denetlemektedir.

Zorunluluk olarak bir dış denetçi tarafından denetlenmekte olan firmanın iç denetim birimi, kendi etkinliğini de iç denetimlerin iç denetim raporuna uygun olarak tamamlanması, iç denetim raporlarının ne kadar sürede hazırlandığı ve iç denetim planı kapsamındaki denetimleri zamanında tamamlayabilme kriterleri ile denetlemektedir

Değer yaratacak riskleri alma ve stratejik hedeflere ulaşmanın sağlanılan en önemli fayda olduğunu belirten risk yönetim müdürü, iç denetimle birlikte ise yasal ve idari düzenlemeler, düzgün kurumsal yönetim prosedürleri oluşturma, paydaş/hissedarlara gerekli bilgileri aktarma ve performans izleme faydalarını da kurumlarına kattıklarını belirtmişlerdir. KRY konusunda yaşanan en büyük sıkıntıları ise Türkiye için yeni olan uygulamada bilgi eksikliği ve model bir yapının olmamasıdır.

Görüşülen ikinci firma da yine bir holding firması olup farklı sektörlerde de faaliyet göstermesinin yanı sıra enerji sektöründe büyük faaliyetler gösteren bir firmadır. Holdingin faaliyetlerinin başlangıcı 25+ yıldır ancak enerjideki geçmişi 11 yıl olup, 18.500 kişi olan istihdam içerisinde de enerji üretimin otomasyona dayanmasından 201-250 arasında kişi enerji sektörüne hizmet etmektedir.

Risk yönetimi birimi altında kurumsal risk yönetim ilkelerini benimseyen kurumun risk yönetiminden uluslararası ilişkiler eğitimi almış risk yönetiminde 10 yıllık bir geçmişi olan risk yönetim direktörü sorumludur. Holding'in bütün riskleri bu birimden yönetilmektedir. 2 yıl önce başlanan risk yönetim çalışmalarının kısmen yerleşik durumda yürütüldüğü firmada üst yönetime raporlama yapan bir raporlama sistemi mevcuttur.

Performans eksikliği ile operasyonların verimliliğinin ve sürekliliğinin sağlanması ve kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ihtiyacı ile başlatılan KRY uygulamasının yürütülmesinde 5 kişi sorumlu olup, bu kişilerin eğitim planları ile bilgi ve becerileri arttırılmaya çalışılmaktadır.

Risk yönetim amaç, çalışma ve taahhütlerini içeren risk yönetim tüzüğüne sahip olmayan kurumda risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, kurum çapında risklerin takip edilmesi ve bir risk yönetim raporlaması ve bilgi sistemi kurmak kurumun yerleştirmeye çalıştığı faaliyetleri arasında olup kurum çapında risklerin kontrol aktiviteleri de planları dahilindedir.

Temel performans göstergeleri, temel risk göstergeleri ve yılda bir yapılan risk haritaları ile belirlenen ve ölçümlenen riskler sayısal yöntemler (VaR, Monte Carlo, vb.) ile desteklenmektedir. Stratejik risklere odaklanmayla başlayan KRY sürecinde önceliğini finansal risklere çeviren firma ikinci sırada da stratejik riskleri ile ilgilenmektedir. Böylelikle hedefledikleri risk yönetim yapısının dışında bir yapı halini alan KRY konusunda hiçbir standardı uygulamamaktadır. Hiçbir harici danışmanlık hizmeti de almayan risk yönetim bölümü kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını üç ayda bir gözden geçirmektedir.

Holding çapında iç denetimi olan ancak bunu enerjideki firmasına uygulamayan kurumun risk yönetim faaliyetinden sağladığı faydalar; değer yaratacak riskleri alma, stratejik hedeflere ulaşılma, karlılığın artması, yasal ve idari düzenlemeler ve düzgün kurumsal yönetim prosedürleri oluşturmadır. Bazı sistem ve yazılımların kurulması, konuyla ilgili insan kaynağı sağlama, risk yönetim sistemini kurma maliyeti ve kurumsallaşma eksikliği karşılaşılaşın zorluklar arasındadır.

Kurumsal risk yönetimini tamamen yerleşik duruma getiren, ve birebir görüşmelerle uygulamalarındaki bilgileri aldığımız sonuncu kurum yüzden fazla ülkede 120,000 çalışanıyla hem uluslararası hem de Türkiye'nin kamu ve özel sektör sanayi alanındaki

müşterilerine hizmet sağlayan, dünyada lider bir kuruluştur. Türk elektrik ve endüstri piyasalarına 1940'lı yıllardan beri faaliyetini sürdürmektedir.

ABD'deki merkezine bağlı olarak Türkiye'de de risk yönetim faaliyetleri sürdüren firmada risk yönetiminden işletme eğitimi almış, risk yönetiminde 3 yıllık bir deneyimi olan iç kontrol&risk yönetim müdürü sorumludur. Tüm gerekli bilgiler kendisinden görüşmeler sonucu elde edilmiştir. Ayrıca bu bölüme yönetim sistemi (Management System) adlı bölüm de destek vermektedir. ABD merkezinde risk yönetim yapılanmasının geçmişi tamamen yerleşik durumda olarak çok uzun yıllara dayanmaktadır. Firmanın Türkiye'deki örgütünde risk yönetim yapılanmasının geçmişi ise 3 yıldır. ABD merkezli olmasından dolayı SOX yasalarına tabi olan kurum, COSO çerçevesi ve OECD kurumsal yönetim ilkeleri (OECD principles of corporate governance)'ne de uyum sağlamaktadır.

Yasal zorunluluklar (özellikle SOX), kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ve daha etkin iç denetim&kontrol ihtiyacı ile KRY çalışmalarına başlayan firmanın Türkiye'deki risk yönetim faaliyetlerinin finansal risklerle olan kısmını bir kişi operasyonel risklerle ilgili kısmını bir kişi yönetmektedir. Çevresel ve en son önem derecesinde ise stratejik risklerine de odaklanılmaktadır. Bunlar dışında ana görevi risk yönetimi olmayan 11+ birçok kişi de KRY de etkili olmaktadır. Etkili tüm çalışanlar eğitimlerle desteklenmektedir.

Kurumda yerleşik bir raporlama sistemi bulunmakta ve başta ABD'deki merkezi risk yönetimi olmak üzere üst yönetim, süreç sahipleri ve dış denetçiye raporlama yapılmaktadır. Ayrıca şirketin tüm çalışanları oluşturulan risk yönetim politikaları ve tüzüğü ile KRY'den haberdar olmaktadır. Soru setimizde yer alan; risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, risk finanslama çözümlerini belirlemek ve uygulamak (hedging uygulayarak), kurum çapında riskleri karşılamak, şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulamak, yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak, bir risk yönetim raporlaması ve bilgi sistemi

kurmak, kurum çapında risklerin kontrol aktiviteleri, kurum çapında risklerin takip edilmesi, şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmak faaliyetleri tamamen yerleşik duruma gelmiştir. Buda KRY'nin kurumda tam etkin çalıştığını gösterir. Temel performans ve temel risk göstergeleri, iç değerlendirme ve yılda bir yapılan risk haritaları ile riskler belirlenip ölçümlenmektedir.

Harici danışmanlık hizmetlerine başvurmayan risk yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını yılda bir gözden geçirmekte ve hedefledikleri KRY yapısına uygun faaliyet gösterdiklerini belirtmektedirler.

İç denetim ile ilgili üst düzey risk komitesinde CFO vardır ve risk yönetim ve iç kontrol'ün aynı bölümde entegre bir şekilde sürdürülmesi nedeniyle iç denetimden görevli yönetim risk yönetiminden de sorumludur. Ve ayrıca iç kontrol gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetlemekte ve işletmenin varlıklarının ve kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını değerlendirmekte olup finansal denetime en üst sırada önem vermektedirler. Ardından uygunluk ve iş/süreç geliştirme ve en son sırada da danışmanlık işlevleri önemli konumdadır. 150 kontrol aktivitesinse sahip risk yönetim&iç kontrol birimi etkinliğini iç denetim raporlarını ne kadar sürede hazırladığı, iç denetim planı kapsamındaki denetimleri zamanında tamamlayıp tamamlayamadığı kriterleri ile ölçmektedir.

Uyguladıkları yönetim ile kurumlarına, başta süreç geliştirme/iyileştirme olmak üzere stratejik hedeflere ulaşma, yasal ve idari düzenlemeler, düzgün kurumsal yönetim prosedürleri oluşturma, paydaş/hissedarlara gerekli bilgileri aktarma, performans izleme, karar mekanizmalarının ve iletişim ağlarının netleşmesi konularında değer katmaktadır. Kuruma KRY sürecini entegre ederken ve uygularken karşılaşdıkları en büyük zorluk insanların değişkenliğe verdiği tepki olmuştur. Risk yönetiminde insan kaynağı ihtiyacı ve risk yönetimine uygun yapılanma değişikliğinin gerektirdiği finansal kaynakları da firma karşılamak zorunda kalmıştır.

Telefon görüşmesi ile bilgilerini aldığımız firma 160 yılı aşkındır Türkiye enerji sektöründe faaliyet göstermektedir. Merkezi Almanya'da bulunan firmanın 190 ülkede

yaklaşık 470.000 çalışanı bulunmaktadır. Böylesine büyük bir kurumun Türkiye'de de risk yönetimini içeren bir organizasyonu mevcuttur.

Kurumsal risk yönetimiyle, destek birimlerindeki denetim (controlling) birimi altında 5 yıldır risk yönetimi üzerinde çalışan işletme eğitimi almış kontrolör (controller) pozisyonundaki kişi ilgilenmektedir. Tüm bilgiler bu pozisyondaki kişiden telefonda uzun bir görüşme sonucunda alınmıştır. Bu birim operatif birimler ile paralel, destek birimleri içerisindedir ve üst yönetimdeki hazine bölümünün altında faaliyet göstererek hazineye raporlama yapmaktadır. Ayrıca gerek görüldükçe de Almanya'daki merkezden destek alınır. Almanya'da uzun süredir yerleşik olan faaliyet Türkiye'de 5 yıldır tamamen yerleşik durumda işlemektedir. Almanya'daki formel yapıya uyumu sağlayıcı şekilde yasal zorunluluklarla başlatılan faaliyete kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ve operasyon verimliliği ile sürekliliğinin sağlanması ihtiyacı da etki etmiştir. Kontol, risk yönetimi ve denetim ile ilgili 20 kadar kişi çalışmakta ve tüm bu çalışanların bilgi ve becerileri eğitim planları ile desteklenmektedir. Risk yönetimi ile ilgili amaç, bilgileri ve taahhütleri belirleyen resmi bir doküman olan risk yönetim tüzüğü vardır ve şirketin tüm çalışanlarına bildirilmiştir.

Risk yönetim prosesini ve/veya fonksiyonunu organize etmek, kurum çapında riskleri belirlemek, kurum çapında riskleri değerlendirmek, risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek, risk finanslama çözümlerini belirlemek ve uygulamak, kurum çapında riskleri karşılamak, yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak, bir risk yönetim raporlaması ve bilgi sistemi kurmak, kurum çapında risklerin kontrol aktiviteleri, kurum çapında risklerin takip edilmesi, ve şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmak faaliyetlerini şirketin uygulamalarına yerleştirilmiştir denilmiştir. Tüm bu faaliyetleri yürütürken kullandıkları tek bir gösterge vardır bu da iç değerlendirmedir.

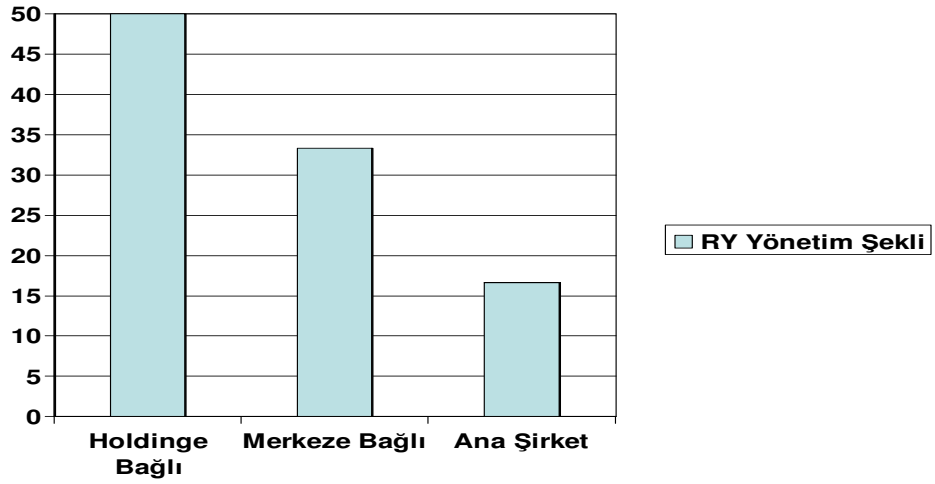
Operasyonel risklere ağırlıklı olarak odaklanan birim ardından önem sırasına göre stratejik, finansal ve çevre risk gruplarına da odaklanmaktadırlar. Hiçbir mevzuat veya standarta uyum sağlamayan firmanın kendisine özgü ciddi titizlilikle hazırlanmış kurumsal yönetim ilkeleri mevcuttur. Bu ilkelerde risk yönetimin gerekliliğinden de

bahsedilmiştir. Hedeflenen yapıya ulaşmakta hiçbir harici risk yönetim danışmanlığı almayan firmada iç denetimden sorumlu yönetim kurulu üyesi risk yönetiminden de sorumlu durumdadır. Bu sorumluluk altında, gerçekleştirilen iş ve eylemlerin belirli strateji ve politikalara uygunluğunu ve işletmenin varlıklarının/kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını denetlemekte mevcuttur. Verimlilik ve müşteri odaklılık konularında hassas olan kurumun iç denetim işlevlerinde her türlü denetim bulunmaktadır. Yapılması gereken bir çalışma olarak gördükleri kurumsal risk yönetiminden, değer yaratacak riskleri alma ve karar mekanizmalarının geliştirilme gibi faydalarla geri dönüş almaktadır. Bu yönetim uygulamasını yerleştirirken kurumlarını zorlayacak engellerle karşılaşmamışlardır.

10.4 Araştırma Sonuçları

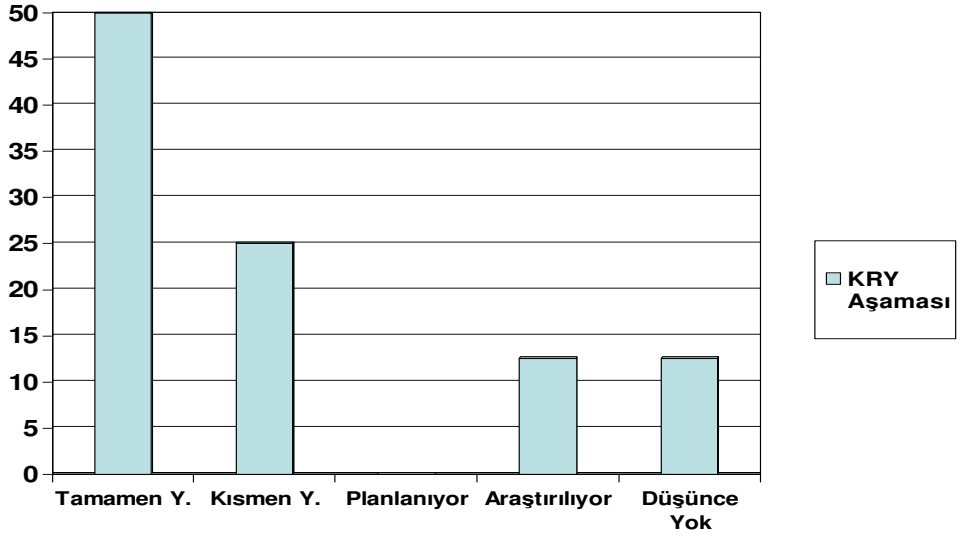
Şirketlerden aldığımız cevaplara göre, enerji sektöründe faaliyet gösteren büyük ölçekli 45 firmanın 13'ünde kurumsal risk yönetim uygulaması ya başlamakta yada tamamen veya kısmen yerleşik konumda devam etmektedir. Enerji firmalarının %28,8'i kurumsal risk yönetimi ile ilgilenmektedir sonucu çıkarılsa da geriye kalan %61,2'si ilgilenmemekte olduğu söylenemez. Bilgi alamadığımız firmalar olduğundan diğerlerinde uygulamaların varlığı veya yokluğu hakkında bir şey söyleyemeyiz. Bilgi alınan 18 firmanın %72,2 si KRY uygulamaktadır denilebilir ancak araştırmamıza bilgi katkısında bulunan firmaların çoğu KRY ile ilgili olduklarından bu sonuç ağırlıklı bir sonuç olarak ortaya çıkmaktadır.

Aldığımız cevaplar doğrultusunda KRY konusunda özel sektörün kamu sektörüne göre daha ilgili ve bilgili olduğu ortaya çıkmıştır. Özel sektörde ise holding şirketlerinde uygulamanın yaygın olduğu, ve genellikle Şekil 10.1' de gösterildiği gibi holdinge bağlı bir orgütlenme ile yönetildiği ortaya çıkmıştır.



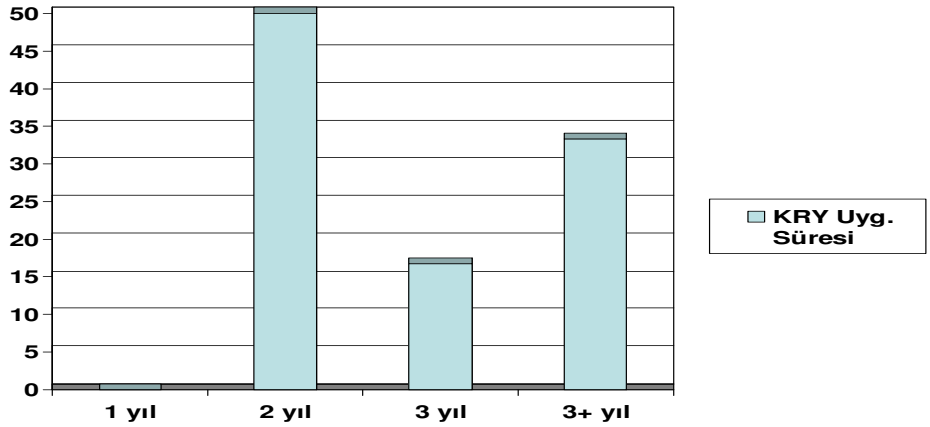
Şekil 10.1 : Risk yönetiminin firmalardaki yönetim şekli

Şekil 10.2'de görüldüğü gibi ankete tam cevap veren şirketlerin yarısı (%50'si) KRY'i tamamen yerleştirdiklerini söyleselerde hala eksiklikleri olan firmalar mevcuttur.



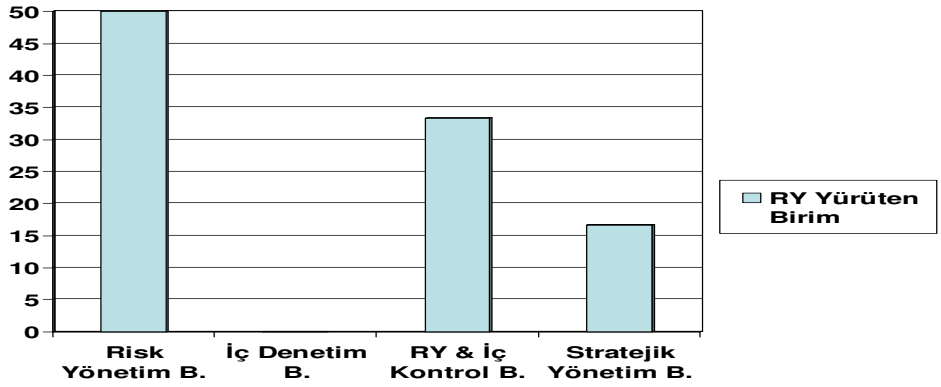
Şekil 10.2 : Kurumsal risk yönetiminin firmalardaki uygulama aşaması

KRY'inin Türkiye enerji sektöründeki geçmişine ortalama 2 yada 3 yıl demek yerinde olacaktır. Şekil 10.3'de ayrıntılı olarak görülmektedir. Bu kadar az geçmişi olan bir yönetim aracının tabiki bilgi ve uygulama modeli açısından eksiklikleri olacaktır.



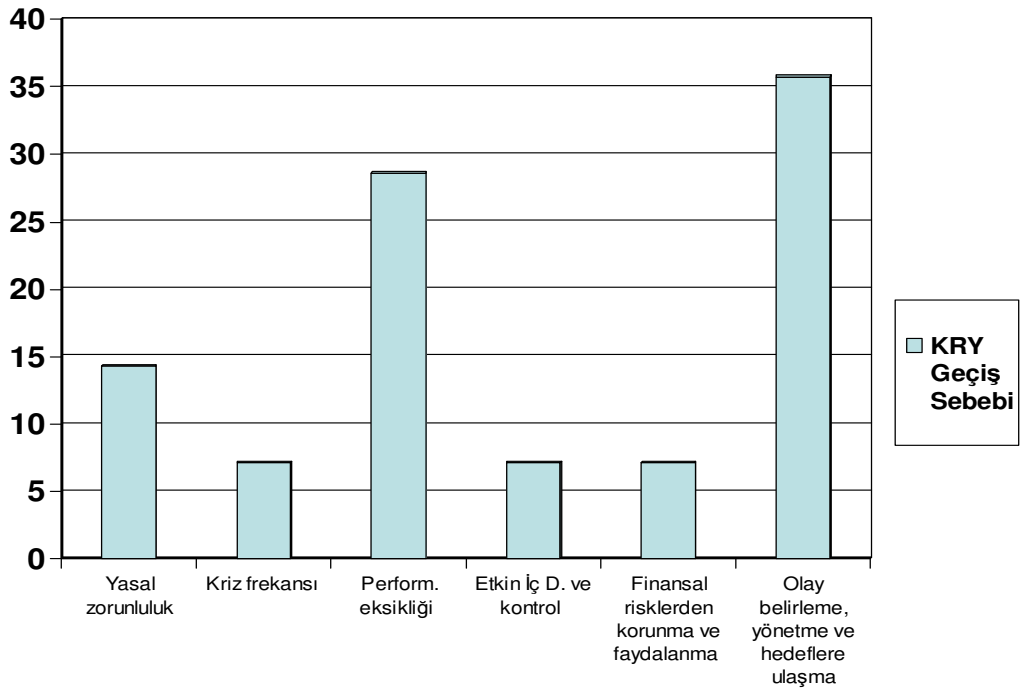
Şekil 10.3 : KRY uygulayan firmaların uygulama süreleri

Birimsel yapılanmada ise risk yönetim adı altında oluşumlar ve iç kontrol ile birlikte oluşmuş risk yönetim&iç kontrol birimleri aynı sayıda olarak Şekil 10.4'de görülmektedir. Türk şirketlerinde risk yönetim ayrı iç denetim ayrı bir yapı mevcutken, yabancı yatırımlı firmalarda iç kontrol ile birleşik bir risk yönetimi göze çarpmaktadır. Bu da daha çok uluslararası yasal zorunluluklara uyma gerekliliğinden kaynaklanan bir durum olabilmektedir.



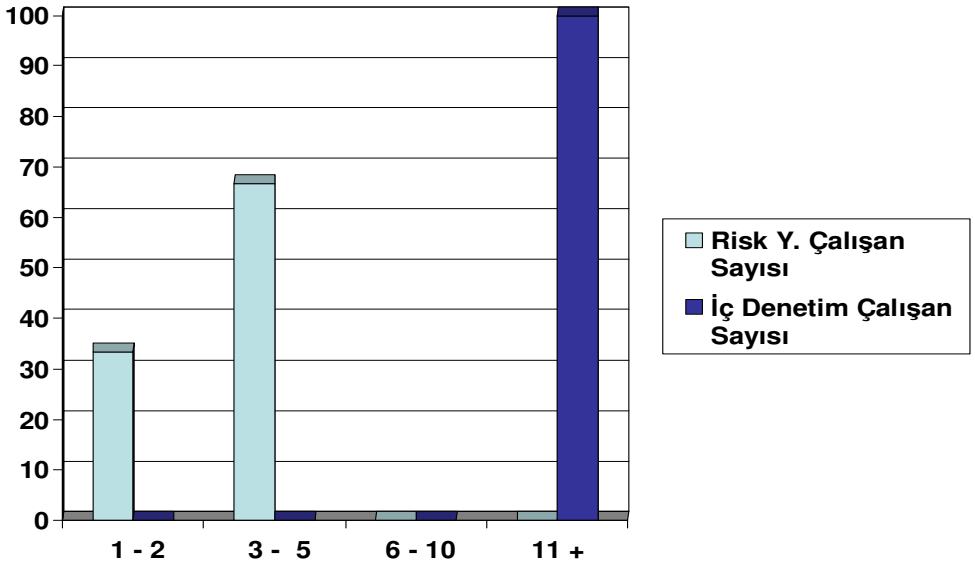
Şekil 10.4 : Risk yönetimini yürüten birimler

En çok, kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ihtiyacı araştırma yapılan firmalarda KRY'e başlama sebeplerinden görülmüştür. Bunu takiben performans eksikliği ile operasyonların verimliliğinin ve sürekliliğinin sağlanması sebebi ikincil önemli etki olarak bulunmuştur. Şekil 10.5'de ayrıntılı sonuçlar mevcuttur.

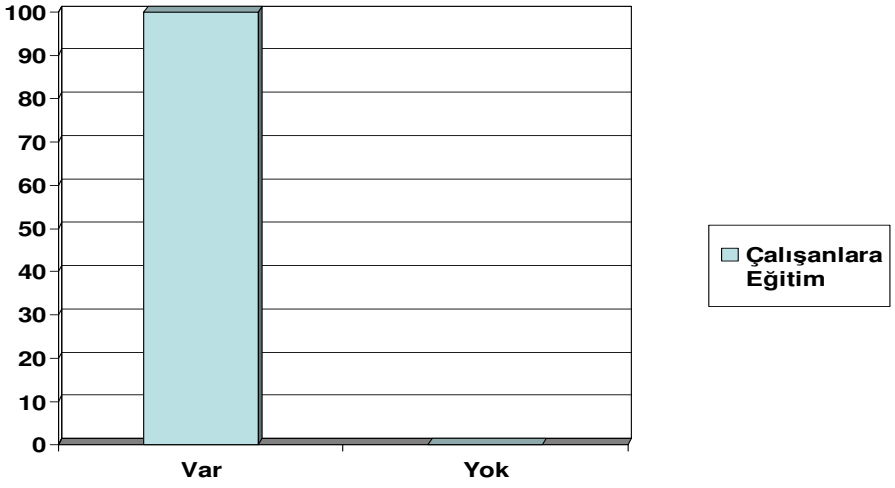


Şekil 10.5 : Firmaların KRY'e geçiş sebepleri

Bu sebeplerle kurumsal risk yönetimine başlayan firmalarda risk yönetimi ile ilgili birimlerdeki kişi sayısının ortalama 3-5 arasında olduğu ortaya çıkmıştır. Şekil 10.6'daki tablo risk yönetimi ve iç denetimdeki çalışan sayılarını göstermektedir. Az sayıda kişinin €olması bu uygulamaların kolay bir uygulama olmasından değil, sürece tüm çalışanların katkı sağlamasından kaynaklanır. Birimlerdeki kişiler uygulamayı yöneten kişilerdir. Bu süreçte ana faaliyeti risk yönetimi olmayan bir çok çalışanda onlara yardım etmektedir. Risk yönetimi çalışanları ve yardım eden diğer çalışanlara eğitim desteği sağlanmaktadır. Şekil 10.7'de gösterilmektedir.

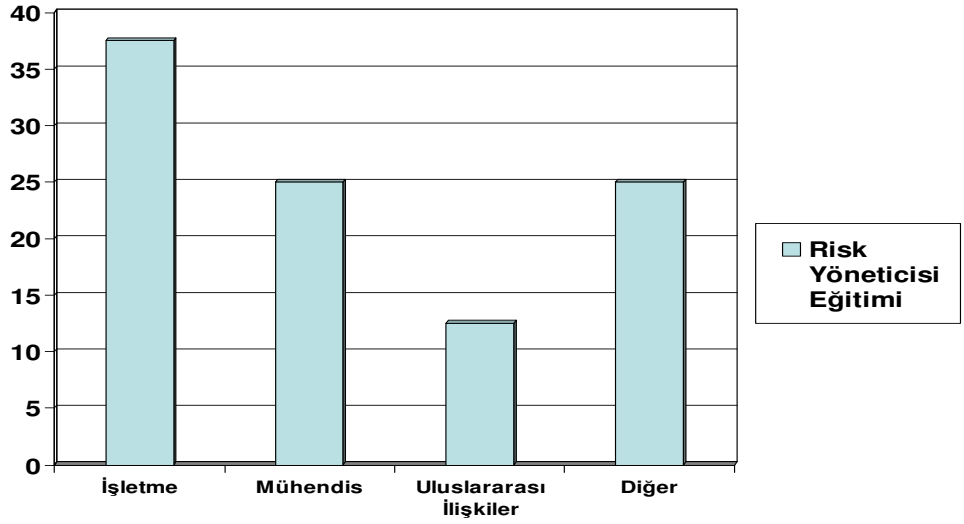


Şekil 10.6 : Risk yönetimi ve iç denetim birimlerindeki çalışan sayıları dağılımı



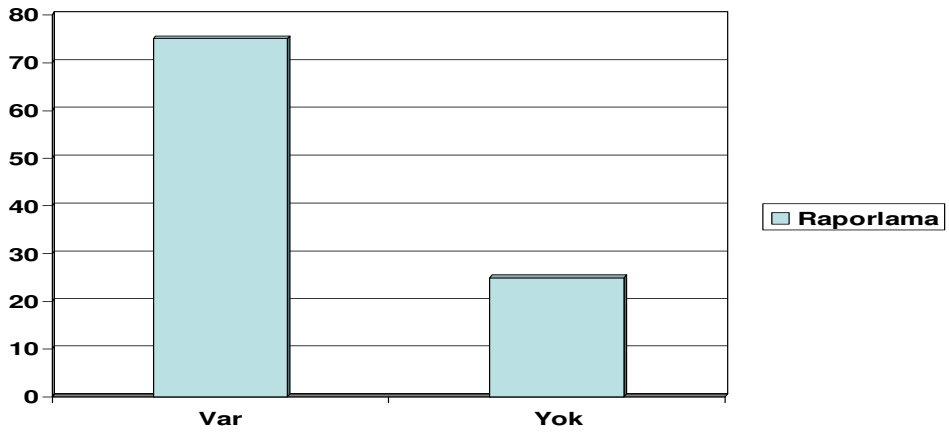
Şekil 10.7 : Çalışanlara eğitim varlığı

Risk yöneticilerinin hangi meslek dalından geldiğine bakılırsa çoğunluğun işletme eğitiminden geldiği görülmektedir. Risk yönetiminde etikili olan diğer eğitim oranları Şekil 10.8'de gösterilmektedir. Risk yönetimindeki deneyimleri ortalama 5 yıldır.



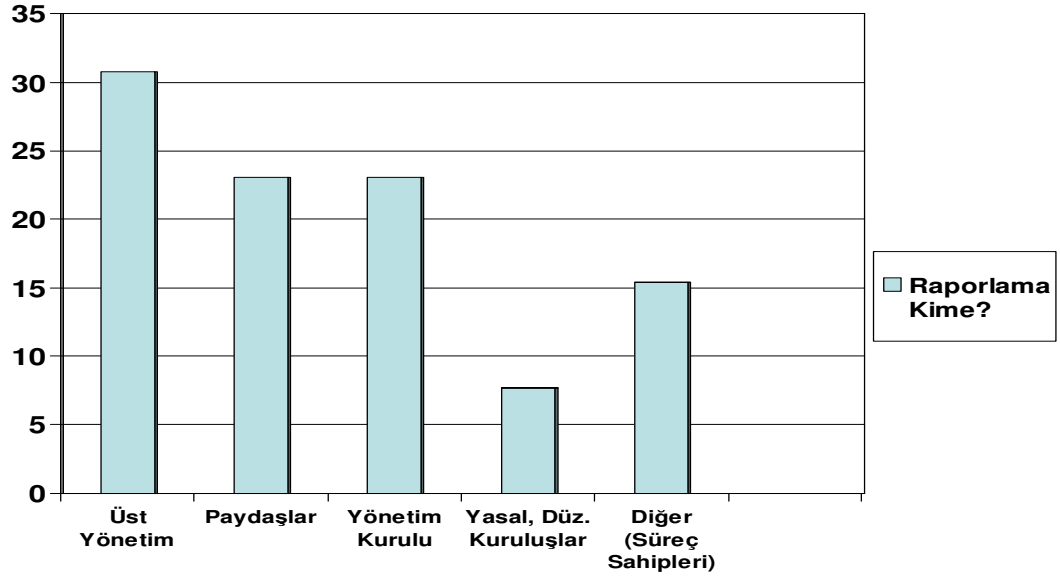
Şekil **10.8 :** Risk yönetcilerinin eğitim durumu

Raporlama sistemi kurumsal risk yönetiminin olmazsa olmazlarındandır, uygulamaya başlayan şirketlerin neredeyse hepsi bu sistemi kurmuşlardır. Raporlama sistemini kuranların oranları Şekil 10.9'da gösterilmektedir.



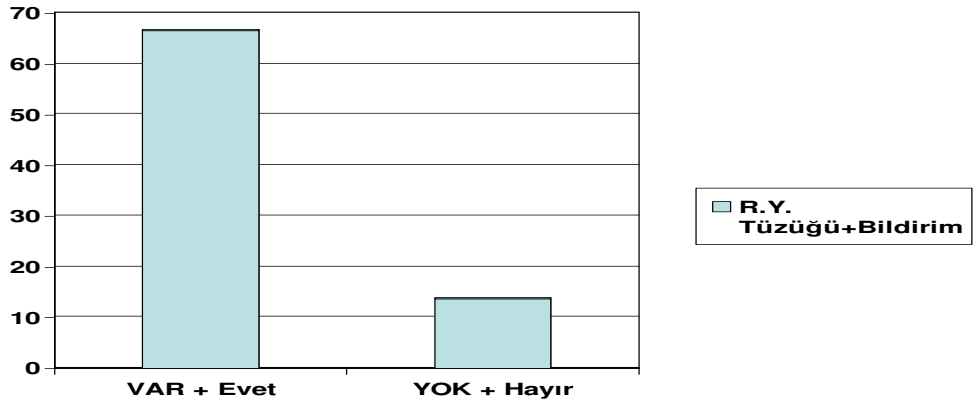
Şekil 10.9 : Raporlamanın varlığı

KRY uygulamasını yapanlar en çok üst yönetim ve yönetim kuruluna raporlama yapmaktadırlar. %37,5'u üst yönetime raporlamalarını yapmaktadır. Şekil 10.10'da raporlamaların hangi oranda kimlere yapıldığı gösterilmektedir.



Şekil 10.10 : Raporlamanın yapıldığı merci dağılımı

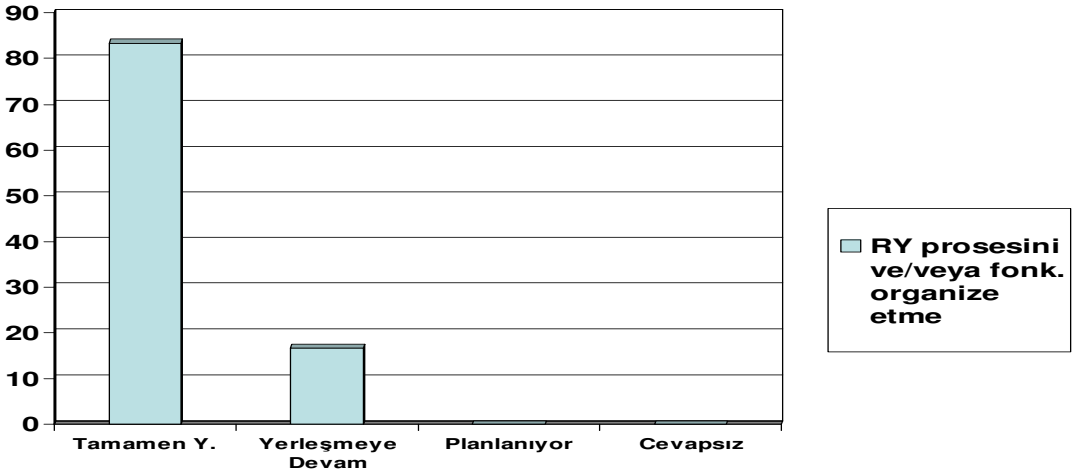
Risk yönetimin amaç, uygulama ve taahhütlerinin belirlendiği risk yönetim tüzükleri (politikaları) şirket çalışanlarını ve kamuoyunu bilgilendirme açısından oldukça önemlidir ve şirketlere klavuzluk yaparlar. Uygulama yapan firmaların %66,6'sı böyle bir tüzüğe sahiptir ve tüm çalışanlarını bu tüzükten haberdar etmişlerdir. Bu oran Şekil 10.11'de gösterilmektedir.



Şekil 10.11 : Risk yönetim tüzüğünün ve bildiriminin varlık oranları

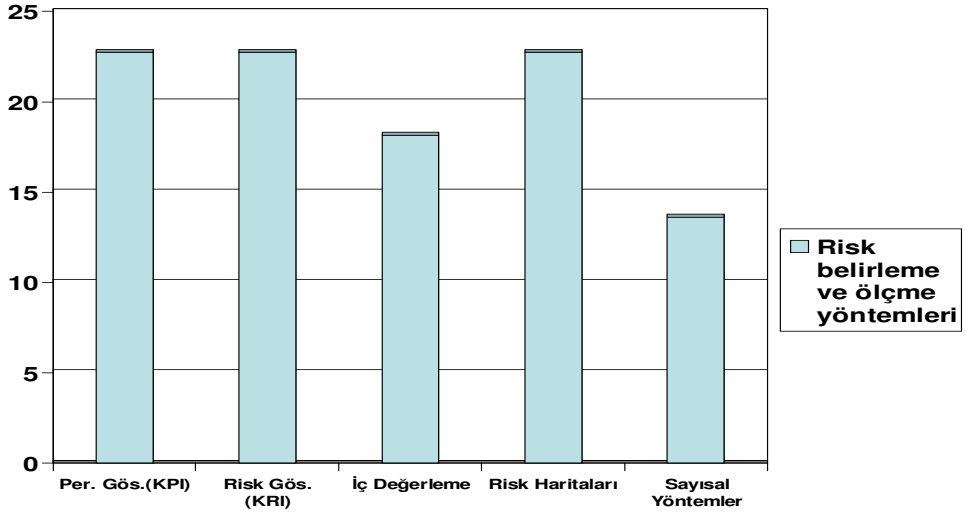
Kurumsal risk yönetim faaliyetlerinden büyük bir kısmı bir çok firmada tamamen yerleşik cevabı ile karşılaşılsada hala düzeltme ve uygulamayı geliştirme çalışmaları devam etmektedir. Özellikle risk yönetim prosesini ve/veya fonksiyonunu organize

etmek, firmalardaki en yerleşik uygulama olarak karşımıza çıkmaktadır. Şekil 10.12'de bu sonucu görmek mümkündür. Yani kurumsal risk yönetimde yetki ve sorumluluklar genel olarak belirlenmiştir, çıkarımı yapılabilir.



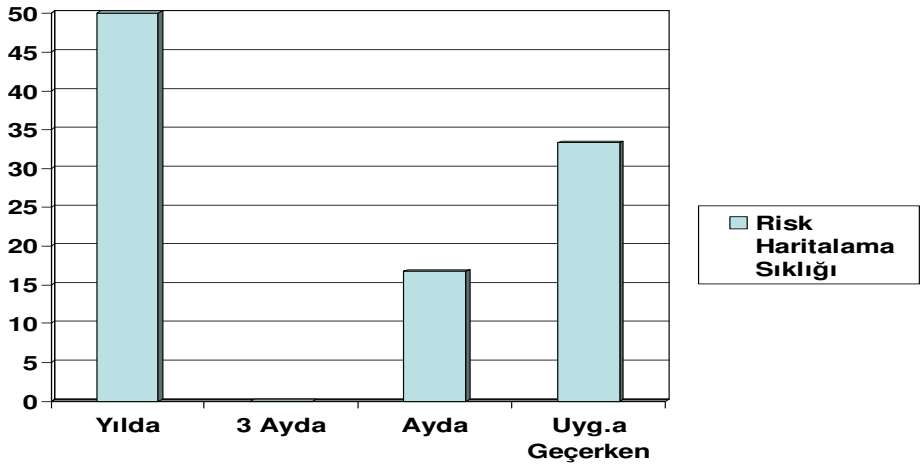
Şekil 10.12 : Risk yönetim prosesi ve fonksiyonu organize etme aşaması

Firmalar risklerini belirlerken ve ölçerken en çok risk haritalarını, performans ve risk göstergelerini kullanmaktadır. Sonuçlar Şekil 10.13'de gösterilmektedir.



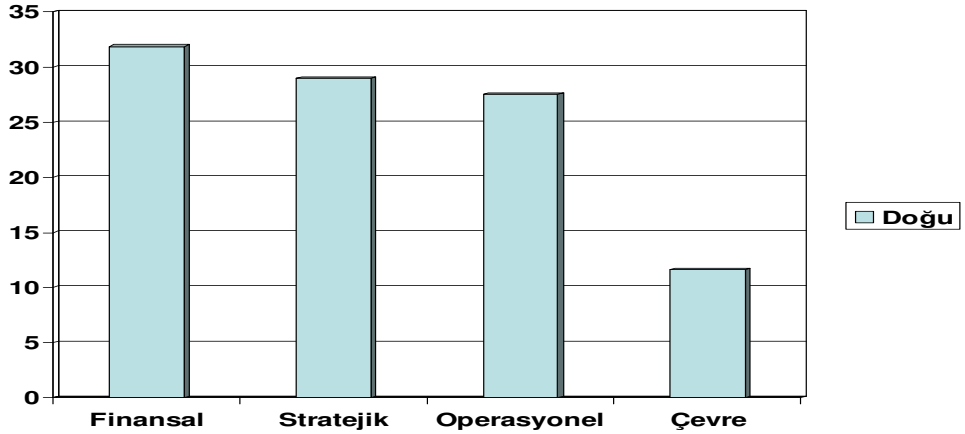
Şekil 10.13 : Risk belirleme ve ölçme yöntemleri

Risk haritalarını belirli periyotlarla güncellemek gerekir. Risk haritaları kullanan firmaların %50'si haritalarını yılda bir güncellemekte, %16,7'sı ise ayda bir güncellemektedir. Sıklık oranlarının dağılımı Şekil 10.14'de gösterilmektedir.



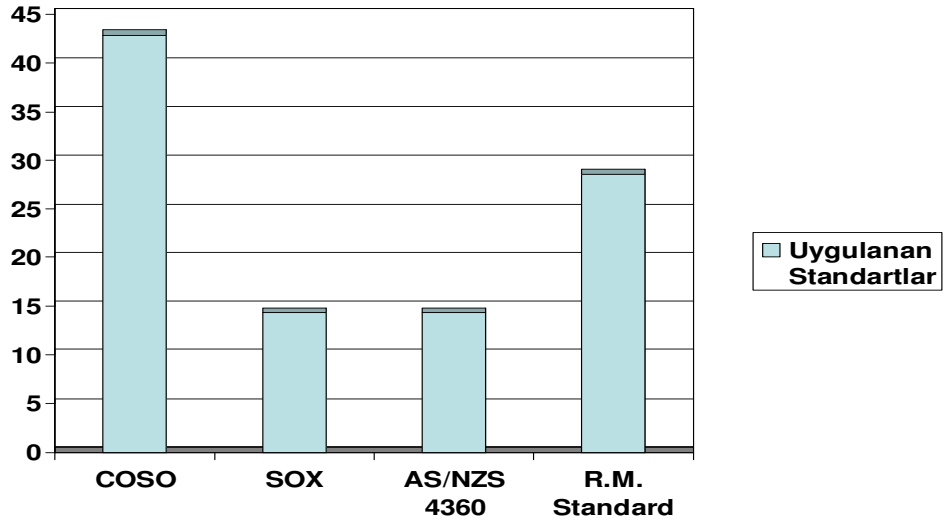
Şekil 10.14 : Risk haritalama sıklık dağılımı

Firmadan firmaya odaklanılan risk grupları değişsede genel bir sonuç çıkarıldığında, finansal riskler firmaların uygulamada en çok önem verdikleri risklerdendir. Hemen ardından ise stratejik riskler önemli görülmektedirler. Bu sıralama Şekil 10.15'de gösterilmektedir.



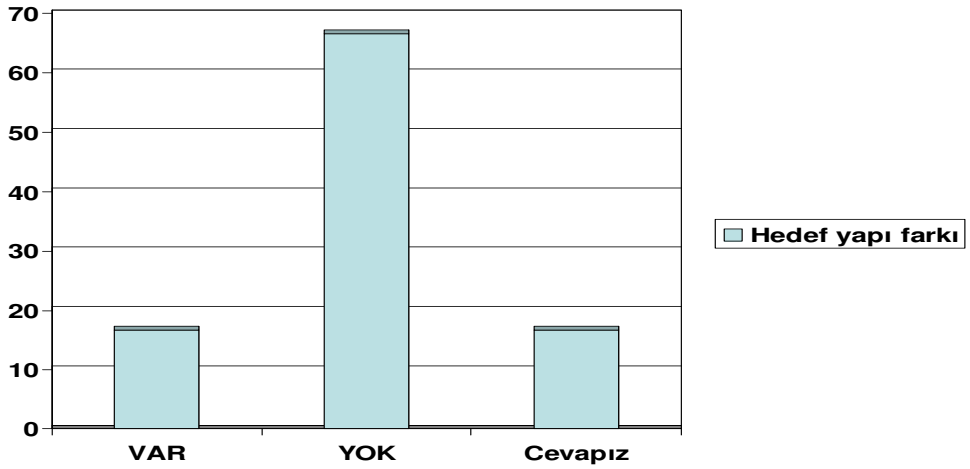
Şekil 10.15 : Risk odaklanma dağılımı

COSO en yaygın olarak kullanılan yasal yapı olarak araştırma sonuçlarında ortaya çıkmıştır. Diğer yasal standartların kullanılma dağılımları Şekil 10.16'da gösterilmektedir.

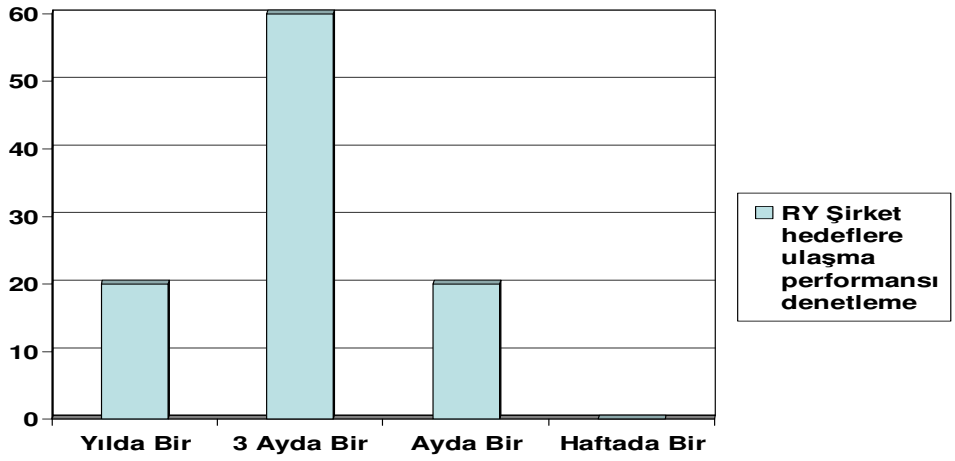


Şekil 10.16 : Firmalarda uygulanan standartların dağılımı

Hedeflenen yapı ile farkın olup olmadığı ankette cevaplayıcılara sorulan sorulardan biridir. Bu sorunun cevapları Şekil 10.17'de görülmektedir. Cevaplayıcıların %66,7'si hedefledikleri kurumsal risk yönetimine uyumlu bir yapıya geldiklerini belirtmişlerdir.

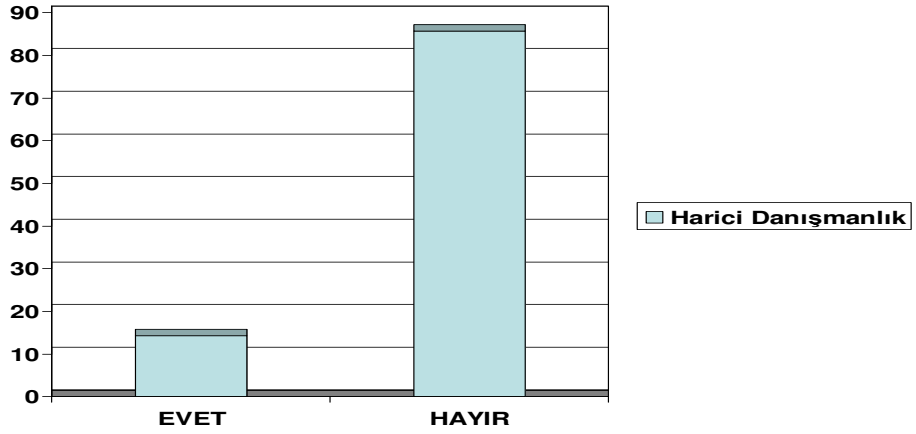


Şekil 10.17 : Hedef yapı ile uygulanan yapı farkı varlığı sorgu cevabı



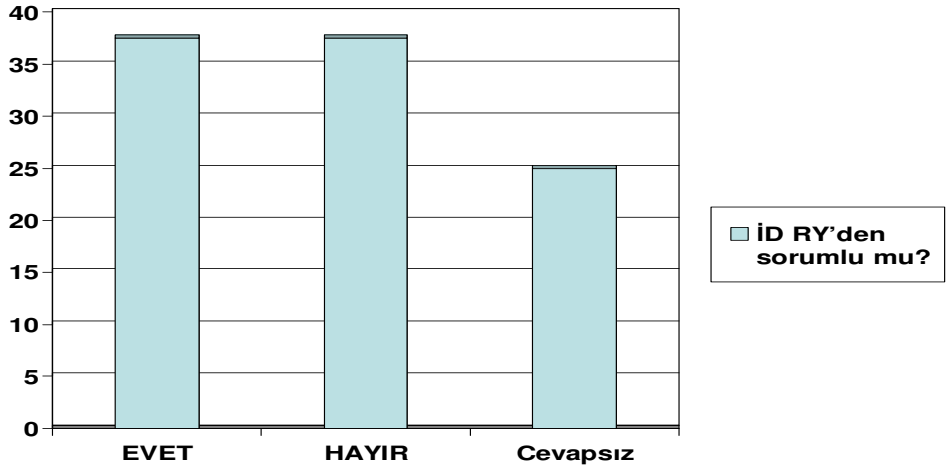
Şekil 10.18 : RY'nin şirket hedeflerine ulaşma performansını denetleme sıklık dağılımı

KRY'i planlayan veya uygulayan firmaların yanlızca %14,3'ü (bir tanesi) uygulama dönüşüm sürecinde kurumsal risk yönetim konusunda harici bir danışmanlık almıştır.Verilen cevapların dağılımı Şekil 10.19'da gösterilmektedir.



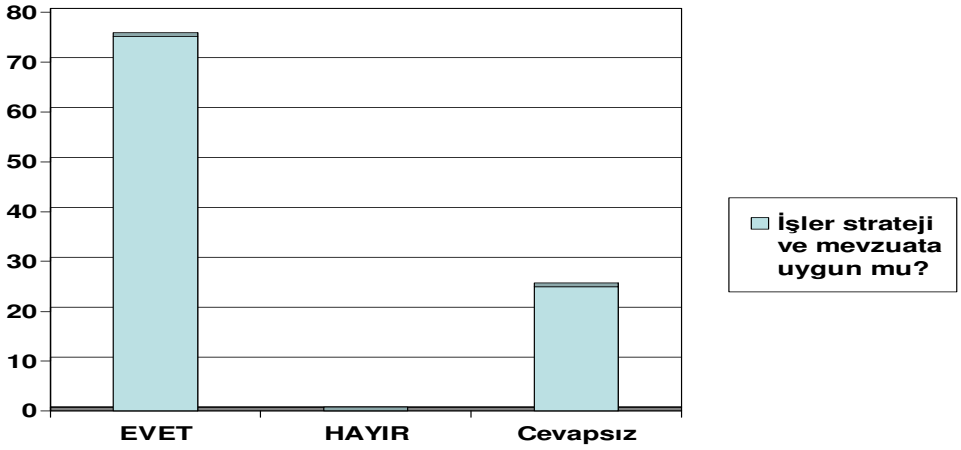
Şekil 10.19 : KRY'ni firmaya entegre ederken harici danışmanlık alma

Araştırmanın son kısmında risk yönetimi ve iç denetim arasındaki ilişki sorgulanmıştır. Ve cevaplayıcılardan üç tanesinde iç denetimden sorumlu yönetim kurulu üyesi, risk yönetiminden de sorumludur. Cevap oranları dağılımı Şekil 10.20'de gösterilmektedir.

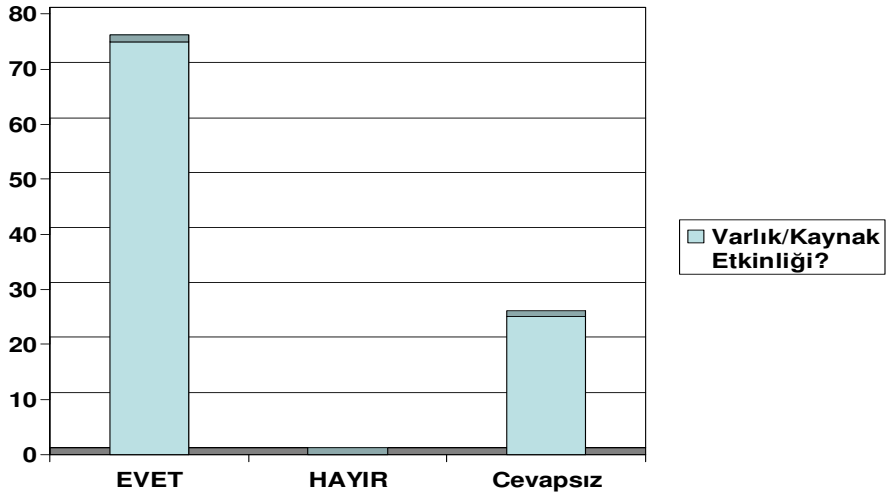


Şekil 10.20 : İç denetimin RY'den sorumluluğunun varlığı

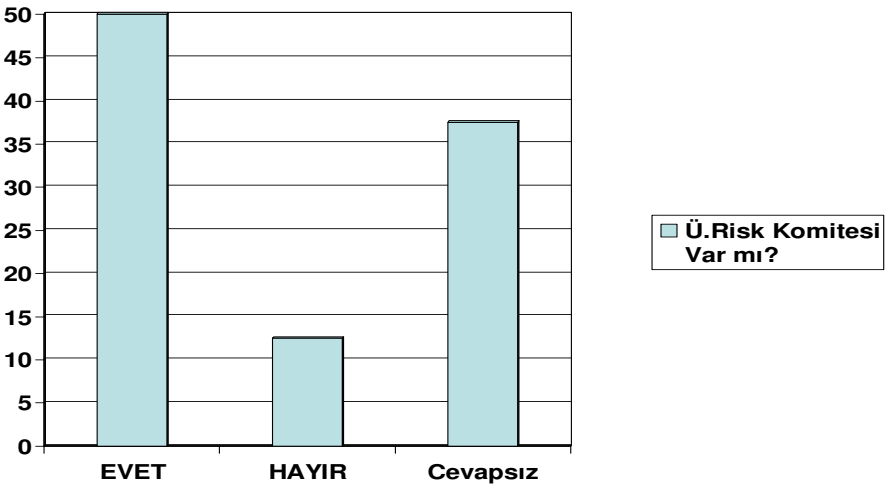
Araştırmamıza katılan firmalarda da iç denetim, gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetleyerek risk yönetimine katkıda bulunmakta ve üst düzey risk komitelerinde yer alarak risk yönetimi ile ilişkilerini göstermektedirler. Ayrıca varlık/kaynak etkinliğinde de aktif rol oynamaktadır. Tüm bunlar soru setinde cevaplayıcı firmalara sorulmuştur. Cevapların ayrıntılı dağılımı Şekil 10.21 Şekil 10.22 ve Şekil 10.23'de gösterilmektedir.



Şekil 10.21 : İşlerin strateji ve mevzuata uygunluğunun varlığı

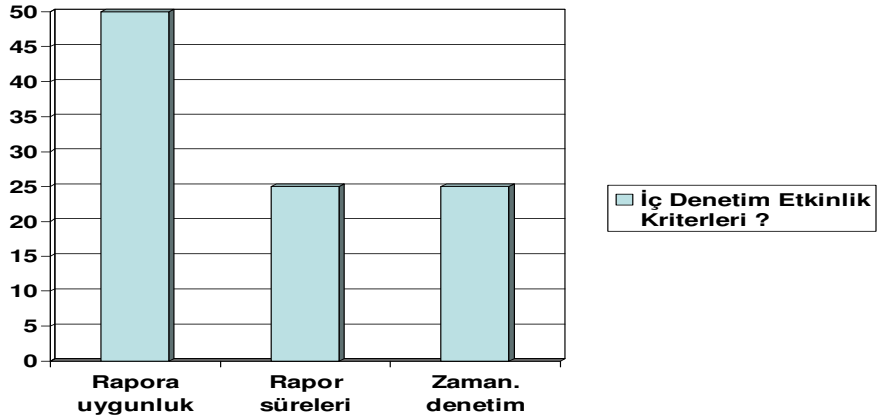


Şekil 10.22 : İç denetimin varlık/kaynak etkinliği görevi varlığı



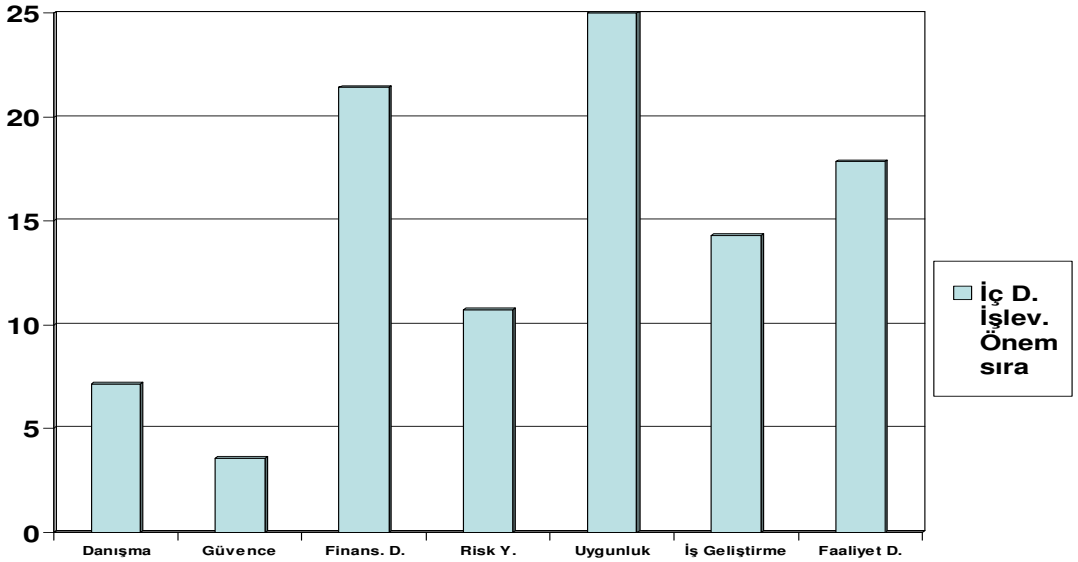
Şekil 10.23 : Üstdüzey risk komitesi varlığı

İç denetim kendi etkinliği ölçerek de karşılaşılabilecek risklerle daha iyi baş edebilmektedir. Kendi etkinliğini ölçmede kullanılan kriterler sorulduğunda Şekil 10.24'deki cevap dağılımları ile karşılaşılmıştır.



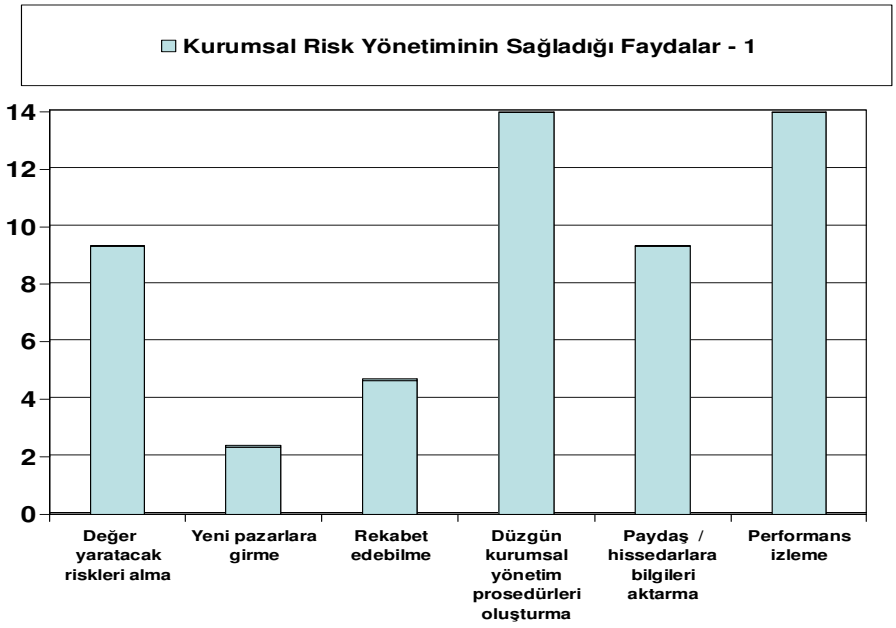
Şekil 10.24 : Kullanılan iç denetim etkinlik kriterleri

İç denetimlerin asli görevleri araştırmamız sonucuna göre uygunluk denetimidir. Ancak diğer görevleri de Şekil 10.25'de verilen cevap dağılımları ile birlikte gösterilmektedir.

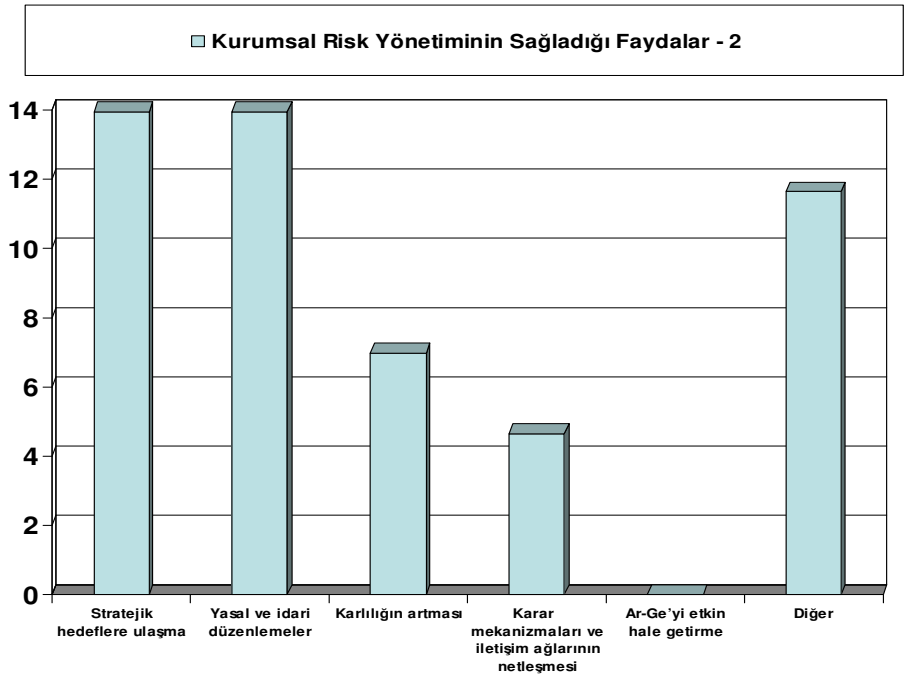


Şekil 10.25 : İç denetim işlevleri önem sırası dağılımı

Araştırmada, düzgün kurumsal yönetim prosedürleri oluşturma, performans izleme ve stratejik hedeflere ulaşılma firmaların KRY'den sağladıkları en önemli faydalar olarak ortaya çıkmıştır. Çıkan tüm sonuçlar Şekil 10.26 ve Şekil 10.27'de görülmektedir. Ortaya çıkan fayda sonuçları "7th Annual Global CEO Survey" adlı araştırmada çıkan faydalar ile de örtüşmektedir.



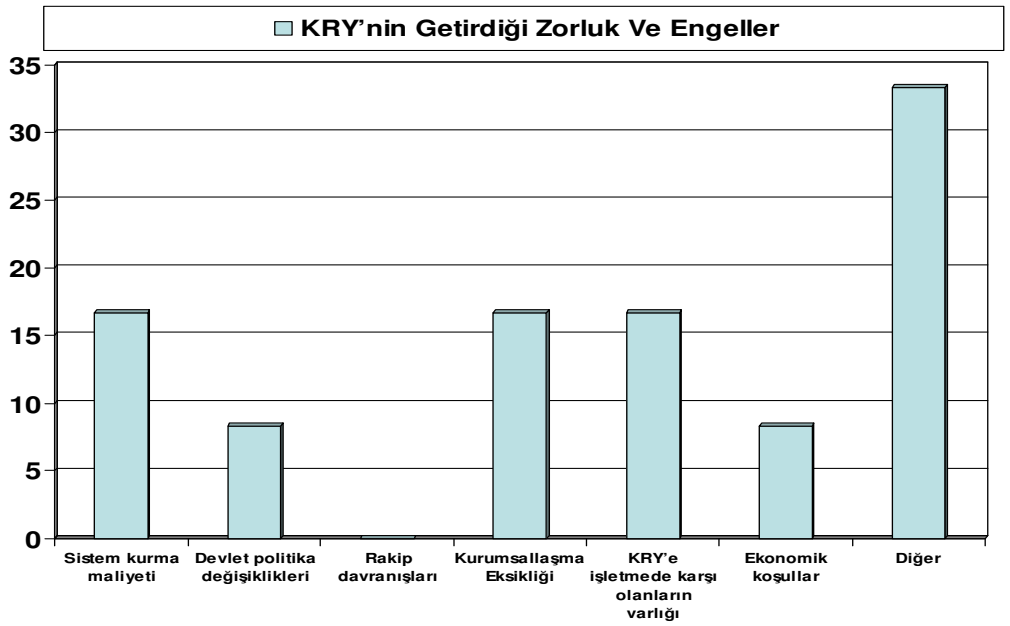
Şekil 10.26 : Kurumsal risk yönetiminin sağladığı faydalar – 1



Şekil 10.27 : Kurumsal risk yönetiminin sağladığı faydalar - 2

Karşılaşılan en önemli zorluklar ise aynı önem derecesinde olmak üzere risk yönetim sistemini kurma maliyeti, kurumsallaşma eksikliği, risk yönetimine işletme içinde karşı

olanların varlığı ve KRY konusunda bilgi eksikliğidir. Bu zorlukların hepsi Türkiye'nin ekonomik yapısından ve kurumsal risk yönetimindeki durumundan kaynaklanmaktadır.



Şekil 10.28 : Kurumsal risk yönetiminin getirdiği zorluk ve engeller

Dünyaya kıyasla Türkiye'de hiçbir zorunluğunun olmadığı kurumsal risk yönetim alanında enerji sektöründeki firmaların her nekadar çok bilgi vermeselerde gönüllü oldukları yargısını çıkarmak mümkündür. Türkiye'de hala şeffaflığın tamamiyle oluşmamasından kaynaklı firmalardan bilgi almak mümkün olmasada, araştırmadan anlamlı ve tutarlı sonuçlar çıkarmak mümkün olmuştur. Soru setinde bulunan sorulara verilen tüm cevaplar Ek A.2'de verilmektedir.

KRY ikinci olgunluk seviyesi, genel uygulamaları kapsamaktadır. Bu seviyede kurum içinde risk yönetimi anlaşılırlığı sağlanmaya başlanmış ve olay bazlı bilgi akışı elde edilmektedir, Türkiye enerji sektründeki uygulamalar bu seviyenin üstündedir ancak üçüncü olgunluk seviyesine de tamamen ulaşmış değildir. Üçüncü olgunluk seviyesinde bulunan organizasyonlar, KRY uygulamalarında bugünün en iyi uygulamalarını gerçekleştirmektedirler. Türkiye enerji sektöründeki KRY uygulamaları için bugünün en iyi uygulamaları arasındadır çıkarımı yapmak doğru olmaz. Bu nedenle Türkiye enerji sektörünün uygulamaları ikinci olgunluk seviyesi ile üçüncü olgunluk seviye arasındadır demek yerinde bir sonuç çıkarım olacaktır.

11. SONUÇ

Risk, iş hayatının ayrılmaz bir parçasıdır. Kurumların hissedarlarına mümkün olabilen en yüksek değeri sağlayabilmeleri faaliyet göstermekte oldukları tüm iş kollarında karşı karşıya olunan risklerin doğru bir şekilde yönetilmesi ile mümkün olabilmektedir. Birçok şirket artık riski stratejik bir araç olarak görmeye ve riski sistematik olarak yöneterek rekabet edebilme güçlerini sağlamlaştırmaya başlamıştır. Şirketin hedefleri çerçevesinde belirli olayların ya da koşulların tanımlanması, sonuçlarının öngörülmesi ve bunlara karşılık bir strateji geliştirilmesi artık günümüz iş dünyasında sürdürülebilir başarıyı sağlamak için şart olmuştur. Ancak 2008 yılının sonlarında baş gösteren uluslarası krizle birlikte global risk iştahının düşmesi şirketleri risk almaktan uzağa sürüklemektedir. Böylece başarısızlık en sık karşılaşılan terim haline gelmektedir.

Risk yönetimi, kurumsal yönetimin en temel unsurlarından biri olmuştur. Özellikle kurumsallaşma isteği doğrultusunda, KRY kurumsallaşma yolundaki adımlardan biri olarak görülmektedir. Şirketlerin kurumsallaşırken şeffaf, strateji ve performans beklentileri belirlenmiş, etkin yapılanmış olması gerekir. Kurumsallaşma sürecinde şirkete duyulan güvenle birlikte belirsizlik ortadan kaldırılmalı, çalışanların verimliliği arttırılmalıdır. Tüm çalışanların profesyonelleşmesi hedeflenirken şeffaf ve devamlılık ilkesine dayanan pozitif yaklaşım izlenmeli, şirketin sosyal sorumluluk ve kurum içi iletişim ile yakınlaşması sağlanmalıdır. İşte KRY tüm bu gerekliliklere uygun bir zemindedir.

Özellikle 11 Eylül saldırılarından sonra birçok firma için vazgeçilmez bir konu haline gelen kurumsal risk yönetimine ilginin artması firmaların hem risklerinin farkına varmasına hemde performanslarını arttırmasına olanak sağlamaktadır. Bu olanaklar, tez kapsamında yapılan araştırmada da ortaya çıkan sonuçlardandır.

Enerji ve ekonomik gelişme arasında kuvvetli bir ilişki olduğu bilinmektedir. Endüstrileşmiş ülkeler ekonomilerinin gelişmesine, nüfus artışına, dünya enerji arzı ve talebine göre enerji politikalarını oluşturmaktadırlar. Son 20 yılda, başta Avrupa ülkeleri olmak üzere, Dünya çapında yaşanan enerji sektörünün serbest piyasa ortamında rekabete açılması ve oluşturulan piyasanın düzenlenmesi ve denetlenmesi süreci, ülkemizde de enerji sektörünün yeniden yapılandırılması ve düzenlenmesi ihtiyacını beraberinde getirmiştir. Enerjinin elektrik, petrol, doğalgaz gibi tüm alanlarında bütüncül yaklaşımla değer zinciri oluşturacak şekilde eğilim göstermesi de gerekmektedir. Bu süreç birçok riski beraberinde taşımakta ve bu risklerin yönetilebilmesi sistemli ve disiplinli bir yönetsel yaklaşım olan KRY'ni gerekli kılar.

Türkiye'deki enerji işletmelerinin bu gerekliliğin farkına varmış olmaları ve ilgili çalışmalara başlamış olmaları çok önemli bir gelişmedir. Bu çalışmaların uygun ve sistemli şekilde sürdürülmesi gerektiği öngörülmektedir.

Ülkemizde risk yönetimi, ağırlıklı olarak finansal sektörle anılan bir yönetsel yaklaşım olsa da, yakın gelecekte tüm işletmelerin dolayısıyla enerji işletmelerinin risk yönetimine ağırlık vermeleri kaçınılmaz olacaktır. Uluslararası alanda ülke olarak rekabetimizde risk yönetimi uygulamalarında ilerleme kaydetmeksizin başarı sağlanamayacağı öngörülmektedir.

KRY'nin uygulama modeli ve kapsamı işletmenin faaliyet gösterdiği endüstriye, insan kaynakları ve teknik altyapısının yeterliliğine, faaliyetlerinin karmaşıklık düzeyine, stratejik hedeflerine, büyüklüğüne, faaliyette bulunduğu coğrafyaya ve işletme ortaklarının risk iştahları ile tolerans düzeyine yakından bağlıdır. Her işletme kendi durumunu ve hedeflerini dikkate alarak kendisi için en uygun modeli geliştirmek zorundadır. Enerji sektörünün aktif yapısından kaynaklanır şekilde Türkiyedeki enerji firmaları da bu zorunluluğa uymaları dünyadaki KRY standartlarına ulaşmaları açısından önemlidir.

Türkiye'de kurumsal risk yönetimine olan farkındalığı artırmak, bu alanda yapılan bilimsel çalışmalar ve Türkiye'nin en büyük yapılı şirketlerinin bu uygulamalarını benimsemeleri ile ancak artacaktır. Bu konuda gönüllülerin oluşu da Türkiye'de kurumsal risk yönetimin geleceği için umut vaat etmektedir.

KAYNAKLAR

Aabo, T., **John, R. S**., **and Betty, J. S.,** 2005. The Rise and Transformatıon of The Chief Risk Officer: A Success Story on Enterprise Risk Management, *Journal of Applied Corporate Finance*, (revised version).

Aksel, K., 2002. Kredi Risklerinin Ölçümünde Kullanılan Yöntemler, *Active Dergisi*, No:26.

Andaç, M., İsig Risk Değerlendirme, <*http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh276.ppt.*>, alındığı tarih 23.10.2008.

Apgar, D., 2006. *Risk İntelligence*. Harvard Business School Press, Boston, Massachusetts.

Atamer, M., 2006. Halka Açik Anonim Şirketlerde Kurumsal Yönetim Ve Doğrudan Yabanci Yatirimlar Açisindan Değerlendirilmesi, Uzmanlik Tezi, Şubat, Ankara, Hazine Müsteşarliği.

ATO, Ankara Ticaret Odası, BASEL II Nedir?: Yol Haritası ve KOBİ'lere Etkisi <*http://www.atonet.org.tr/yeni/files/_files/MEDYA_ILISKILERI/baseliki/ato_basel.pdf*>, alındığı tarih 08.04.2008.

Australian/New Zealand Standard, **AS/NZS 4360,** 2003. Risk Management Standart.

AS/NZS 4360, 2004. Risk Management, available from Standards Australia and Standards New Zealand.

Bartelink, R.G.M., 2008. Risk Yönetimi ,RO EMIA CIA CCSA CGAP.

Beasley, M. S., Clune, R., and Hermanson, D. R., 2005. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation, Journal of Accounting and Public Policy 24, 521–531.

Chapman, R.J., 2006. Enterprise Risk Management: Simple Tools and Techniques for Enterprise Risk Management, 07 April, John Wiley & Sons Ltd. Page 30-35.

Collier, P. M., Berry, A. J., and Burke, G. T., 2007. Risk and Management Accounting: Best Practice For Enterprise-Wide Internal Control Procedures, CIMA/Elsevier, Oxford 160pp., Christine Helliar, University Of Dundee, UK.

Colquitt, L. L., Hoyt, R. E., and Lee, R. B., 1999. Integrated risk management and the role of the risk manager. Risk Management and Insurance Review 2, 43–61.

COSO, 2004a. Enterprise Risk Management-Integrated Framework, 16 Temmuz, S.58.

COSO, 2004b. The Committee Of Sponsoring Organizations Of The Treadway Commission, P. 22.

Cömert, N., 2008. Türk Ticaret Kanunu Tasarısı Kapsamında İç Denetim Ve İç Kontrol, *İç Denetim Dergisi* Kış Sayı:21, Marmara Üniversitesi İ.İ.B.F.,İşletme Bölümü.

Cripps, K., 2002. Public Relations Industry 2002 Revenue Tables: The Unintended Conseuences Of New Restrictions.

Çolak, E., Kurumsal Yönetim Uyum Ve Raporlama, SPK Daire Başkanlığı <http://www.spk.gov.tr/displayfile.aspx?action=displayfile&pageid=63&fn=63.pdf#31>, alındığı tarih 01.10.2008.

D'arcy, S. P., 2001. Enterprise Risk Management, *Journal of Risk Management of Korea,* 12: 1.

DeLoach, J. W., 2005. Enterprise Risk Management: Practical Implementation Ideas, Protiviti Inc. (Independent risk consulting).

Deloitte Dergisi, 1999-2001 Sayıları.

Delloitte, 2008. Risk Zekasına Sahip Kurum: Doğru uygulanmış kurumsal risk yönetimi, Kurumsal Risk Hizmetleri, Risk Zekası Serisi – 1.

Derici, O., Tüysüz, Z., ve Sarı, A., 2007. Kurumsal Risk Yönetimi Ve Sayıştay Uygulaması, *Sayıştay Dergisi* Sayı 65.

Erdikler, Ş., 2003. Http://Ww.Turmob.Org.Tr/Turmob/Basin/22-01- (4).Html.

Erkan, A., 2008. Kurumsal Risk Yönetimi, Pricewaterhousecoopers Inc.

Eryılmaz, A., J-SOX, Amerikalı Sox'un Yerini Alır Mı?, Kurumsal Risk Hizmetleri, <*http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/JSOX%20_2_.pdf*>, alındığı tarih 12.11.2008.

Fıkırkoca, M., 2003, *Bütünsel Risk Yönetimi*, Pozitif Matbaacılık, Ankara.

FRC, The Financial Reporting Council, Combined Code http://www.frc.org.uk/corporate/combinedcode.cfm <alındığı tarih >01.10.2008

Gartner, <*www.gartner.com/us/risk*>, alındığı tarih 20.04. 2008

Gökalp, F., 2005. Genel Hatları İle Sarbanes Oxley Kanunu Ve Türkiye'deki Şirketlere Etkisi, Ege Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, *Muhasebe Finansman Araştırma ve Uygulama Dergisi*, *Analiz Sayı:5 Yıl:14 Konu:14 Ekim.*

Güneş, Ş., 2006. Finansal Risk Yönetimi Ve Simülasyon Modeli İle Uygulanması, Lisans Bitirme Tezi, Yıldız Teknik Üniversitesi, Endüstri Mühendisliği, İstanbul.

Gürer, H., 2007. *Uluslararası Finansal Raporlama Standartları*, Deloitte Türkiye, 20 Kasım 2007, Swissotel, Ankara

Hampton, **J. J.,** 2008. Governance A Start For ERM. *Business Insurance.* Chicago:**.** Vol. 42, Iss. 4; Pg. 19, 1 Pgs *Insurance Management Society's Glossary,* Jan 28

***IIA*, The Instute of Internal Auditors**, 2004. Applying COSO's Enterprise Risk Management — Integrated Framework*,* September 29 *(* www.theiia.org)

***IIA*, The Instute of Internal Auditors,** Frequently Asked Questions (FAQs) About the Internal Audit Profession. <www.theiia.org>, alındığı tarih 23.07.2008.

***IIA*, The Instute of Internal Auditors,** 2004**.** Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management, September 29, USA.

***IIA-UK*, The Instute of Internal Auditors UK and Ireland**, 2003. Risk based Internal auditing. The I.I.A. UK & Ireland.

IRM, The Institute of Risk Management, **AIRMIC,** The Association of Insurance and Risk Managers and **ALARM,** The National Forum for Risk Management in the Public Sector, 2002. A Risk Management Standard, London.

Karaca, İ., 2007. Unilever ve İç Kontrol, *TIDE XI. Türkiye İç Denetim Kongresi*, 9 Aralık.

Kaya, E.B., 2008, Bir kurumun tepe yöneticisinin bakış açısından iç denetim, http://denetimevreni.blogspot.com/2008/01/bir-kurumun-tepe-yneticisinin-bak_30.html

Kayım, A., 2006, Kurumsal Risk Yönetimi ve İç Denetimin Kurumsal Risk Yönetimindeki Rolü, *Active Dergisi.*

Kazmirci, K., **ve Altunay E.**, 2004. Kurumsal Yönetim Ve Risk Yönetimi, Ernst&Young ve Deloitte Kurumsal Risk hizmetleri 9 Kasım.

Kinney, W. R., 2003**.** Auditing Rısk Assessment And Rısk Management Processes, The Institute of Internal Auditors Research Foundation.

Kishalı, Y., ve Pehlivanlı D., 2006. Risk Odaklı İç Denetim ve İMKB Uygulaması, Nisan, Kocaeli Üniversitesi, İİBF.

Knight, K., 2003. Risk Management: An Integral Component of Corporate Governance and Good Management, *ISO Bulletin*, Ekim.

Korkmaz, İ., 2008. Risk kültürü, *Radikal Ekonomi*, 11 Eylül

Küçük, Y. A., 2007. Havaalanlarında Kurumsal Risk Yönetimi: Atatürk Havalimanı Terminalleri İşletmesi İçin Kurumsal Risk Yönetimi Model Önerisi Doktora Tezi, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Haziran.

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

Madendere, M. A., 2005. Kurumsal Risk Yönetiminde İç Denetimin Rolü, (Çeviri/Derleme), Ekim.

Matyjewicz,G., and D'arcangelo, J. R., 2004. ERM-Based auditing, *Internal Auditing*, Vol. 19, no.6, pp 4-18.

McNamee, D., and Selim, G., 1999. The Risk Management and Internal Auditing Relationship: Developing and Validating a Model**,** *International Journal of Auditing*, 3, s. 171.

Meriç, Z., Kurumsal Risk Yönetimi, *<Http://Www.Elegans.Com.Tr/Arsiv/66/Haber013.Html>,* alındığı tarih 20.06.2008.

Meriç, Z., 2004. Operasyonel Süreçlerde ve Risk Temelli Denetimde Türkiye'deki Kuruluşlar İçin Kurumsal Risk Yönetimi Konusuna Pratik Bir Yaklaşım, *Elegans Dergisi*, (No:66) Mart-Nisan.

Merkley, B. W., and Miccolis, J. A., 2002: Getting left behind. (ERM Survey). (enterprise risk management) (Column). Risk Management 49.4 p28(9). (2427 words), Risk Management Society Publishing, Inc.**,** April.

Murphy, B., and Davies, M., 2001. Enterprise Risk Management, KPMG LLP s1-2

National Audit Office, 2000. Supporting İnnovation: Management Risk in Government Departments, 27 July.

OECD, 2004. OECD Principle of Corporate Governance, 22/04.

OYAK, 2005. Portföy Yönetimi, Aralık.

Pagach, D., and Warr, R., 2007. An Empirical Investigation of The Characteristics of Firms Adopting Enterprise Risk Management, College Of Management North Carolina State University, August.

PWC, Pricewaterhousecoopers Türkiye Danışmanlık Hizmetleri, 2006. Her Yönüyle Kurumsal Risk Yönetimi, Infomag Yayıncılık, S.11.

PWC, Pricewaterhousecoopers, TTK Türk Ticaret Kanunu Tasarısı, Geleceği Hazırlayan Bir Düzenleme <*Http://www.Pwc.com/Tr/Tur/İnsSol/Publ/Ttktasarisi_Tr.Pdf*>, alındığı tarih 12.10.2008.

PWC, Pricewaterhousecoopers, 2004.7th Annual Global CEO Survey Managing Risk**:** An Assessment of CEO Preparedness, New York.

PWC, Pricewaterhousecoopers, Kurumsal Yönetim, Risk ve Raporlama <http://www.pwc.com/extweb/service.nsf/docid/904BB8812EC35CD880257124005539C9>, alındığı tarih> 20.06.2008.

Preston, S. G., and Guy, M. M., 2002. Proactive Risk Management, New York: Productivity Press.

Protiviti Inc. (Independent risk consulting), 2006a**.** Enterprise Risk Management: Practical Implementation Advice, the bulletin, volume 2, issue 6.

Protiviti Inc.(Independent risk consulting), 2006b. Guide to Enterprise Risk Management", Fruguently Asked Questions.

Rasmussen, M., 2006. Teleconference: Monitoring Risk With Enterprise Risk Dashboards Vice President, *Forrester Research*, June 22.

RIMS, Risk and Insurance Management Society Inc. <http://www.rims.org > alındığı tarih 12.06.2008.

Riskactive, 2008. Kurumsal Risk Yönetimi Kurgusu, 15 Nisan.

Saka, T., 2006. Sabanci Holding A.Ş'de Kurumsal Risk Yönetimi, *CRO Raporu*, 9 Mayıs.

Saka, T., 2007. Riski Anlamak ve Yönetmek; Kurumsal Risk Yönetimi, *TKYD Eskişehir İhtisas Programı*, 21 Kasım.

Saltık, N., 2007. İç Kontrol Merkezi Uyumlaştırma Dairesi İç Kontrol Standartları, Maliye Bakanlığı Bütçe Ve Mali Kontrol Genel Müdürlüğü, Ankara.

Sanayi, İç Denetim Uygulamalarında Denetlenecek İç Kontrol Yönetimi, Risk Yönetimi, Performans Yönetimi Ve Yönetişim Sistemleri <http://www.sanayi.gov.tr/download/ic_denetim/ic_denetimin_denetleyece%C4%9Fi_kontrol.pdf>, alındığı tarih 10.12.2008.

SAS, Kurumsal Risk Yönetimi'nde En Önemli Unsurlar:Performans Yönetimi ve Yasal Düzenlemeler **<**http://www.sas.com/offices/europe/turkey/news/pressreleases/june2007/01.htm>, alındığı tarih 10.12.2008.

Sevim, Ş., Çetinoğlu, T., ve Kurnaz, N., 2006. Avrupa Birliği Müzakereleri Sürecinde Ab 8. Yönergesi Kapsamında Türkiye'de Denetim Ve Denetçilik Mesleğinin Durumu: Ab Müzakereleri Gelişim İçin Bir Fırsat Mıdır?, Dumlupınar Üniversitesi İibf.

Serim, A., 2006.10 Soruda Ekonomide Kurumlar, Derecelendirme ve Basel II, *Radikal Gazetesi*, 1 aralık.

Sezer, F., 2005**.** Risk Odaklı Denetim ve Kurumlarda Risk Yönetim Süreçlerinin Değerlendirilmesi, Hazine Kontrolörleri Kurulu Yeterlilik Tezi, Ankara.

Sezgin, C., Risk Yönetimi Bilinci Ve Uygulama Açısından Türk Şirketlerindeki Durum, <http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh301.ppt> alındığı tarih, 10.07.2008.

Shenkir, W. G., and Walker, P. L., 2002. Enterprise Risk Management, CPA, Mcıntire School Of Commerce, University Of Virgina (03 April).

SOX, 2002**.** Sarbanes-Oxley Act**. <***http://www.sarbanes-oxley.com/***>**

Spedding, L. S., and Rose, A., 2007. *Business Risk Management Handbook: A sustainable approach, Director of Research*, SERM Rating Agency, Independent Consultant in Business Risk Management and Due Diligence, and Qualified Lawyer in the UK, EU, India and the USA. September.

SGUL, St George's, University of London, October 2007, Risk Management Policy

Staaiokas, R., and Rupys, R., 2005. Application of Internal Audit in Enterprise Risk Management, Economics of Engineering Decisions, No: 42.

Standard & Poor's, 2008. RatingsDirect: Enterprise Risk Management For Ratings of Nonfinancial Corporations, June 5, The McGraw-Hill Companies.

Süel, U., 2001**.** Kurum Çapında Entegre Risk Yönetimi Deloitte & Touche Risk Yönetim Haber Bülteni Mart/Nisan.

TBB, Türkiye Bankalar Birliği Çalışma Grubu, 2006. Risk Yönetimi Prensipleri, Bankacılar Dergisi, Sayı 57.

TBS, Treasury Board of Canada Secretariat, 2001. Integrated Risk Management Framework, April, s. 10.

TBS,<*www.tbs-sct.gc.ca*>, alındığı tarih 13.09.2008

Tekgül, E., 2007. Kurumsal Risk Yönetimi ve Risk Zekası, Deloitte Türkiye Kurumsal Risk Hizmetleri, *Referans Gazetesi* (Kasım).

Tesla, 2006, Nisan**.** Risk Management Reports.

Tevfik, A.T.,1997. Risk Analizine Giriş,1. Basım, ALFA Kitabevi, İstanbul.

Tillinghast-Towers Perrin Survey, 2006. Enterprise Risk, Management: Trends and Emerging Practices, An ERM Update on the Global Insurance Industry.

Thornton, G., 2003**.** An ERM Framework: Developing Effective Risk Management Strategies to protect your organization, <www.grantthornton.ca>.

TÜSİAD, Türk Sanayicileri Ve İş Adamları Derneği, 2008a. Kurumsal Risk Yönetimi, Şubat (Yayın No. Tusiad-T/-02/452).

TÜSİAD, Türk Sanayicileri Ve İş Adamları Derneği, 2008b**.** Yönetim Kurulları'nda İç Denetim Hakkında Sorulması Gereken 12 Soru (Yayın No: TÜSİAD-T/2008-05-461) Mayıs.

Uğural, A., 2008. Reel Sektörde Kurumsal Risk Yönetimi, Kurumsal Risk Yönetimi ve 2008 Yılı Risk Öngörüleri, Doğuş Grubu Risk Yönetimi, 21 Şubat.

Uzun, A. K., 2007. Aile İşletmelerinde Kurumsal Yönetim Ve İç Denetimin Rolü, Cpa, Cfe, Deloitte.

Ünver, H., Kurumsal Risk Yönetimi**,** Unilever Risk Yönetimi, <http://archive.ismmmo.org.tr/docs/sempozyum/07Sempozyum/09-hasibe%20unver.ppt>, alındığı tarih 10.06.2008.

VBM, 2005. www.ValueBasedManagement.net, 22 Mart.

Vogel, A., 2006. Enterprise Risk Management- SAP AG/30.

Yalçınkaya, T., 2004. Risk Ve Belirsizlik Algılamasının İktisadi Davranışlara Yansımaları, *Muğla Üniversitesi İİBF Tartışma Tebliğleri*, No:2004/05, Muğla.

Yörüker, S., 2007. Kurum Risk Yönetimi Hakkında Tamamlayıcı Ek Bilgiler, Kamu Sektörü İç Kontrol Standartları Rehberi, INTOSAI Mesleki Standartlar Komitesi İç Kontrol Standartları Alt Komitesi.

Yüzbaşıoğlu, A.N., 2003. Risk Yönetimi Ve Bankaların Denetimi ,Risk Yöneticileri Derneği – Finans Dünyası, İstanbul.

Url-1 <*www.knowledge.com*>*,* alındığı tarih 14.08.2008

EKLER

EK A.1

Tamamen bilimsel bir araştırmaya dayanan ve Türkiye'de risk yönetimine genel bakış ve mevcut Risk Yönetimi uygulamaları ve İç Denetim hakkında değerlendirme yapmayı amaçladığımız bu proje dahilinde bizimle paylaşacağınız bilgiler gizli tutulacaktır.
Değerli katkılarınız için şimdiden teşekkür ederiz.

Görüşülen Yetkilinin; Ünvanı/Pozisyonu:

Kurumdaki Mesleki Deneyim Süresi:

Kurumunuzda Risk Yönetiminden Sorumlu Yetkilinin

Öğrenim durumu	
Eğitimini Aldığı Meslek	
Kurumdaki pozisyonu	
Risk Y.deki mesleki deneyimi (Yıl)	

(Tercihlerinizi seçeneklerin yanına "X" işareti koyarak belirtebilirsiniz, çok seçenekli sorularda birden fazla tercihte bulunabilirsiniz.)

İşletmeniz kaç yıldır faaliyetlerini sürdürmektedir?

1-4 yıl	□	10-14 yıl	□	20-24 yıl	□
5-9 yıl	□	15-19 yıl	□	25 yıl ve üzeri	□

İşletmenizde kaç kişi istihdam edilmektedir?

50-100	□	151-200	□	251-500	□
101-150	□	201-250	□	501 ve üzeri	□

1. İşletmenizde risk yönetim uygulaması var mıdır?
VAR YOK
VAR ise hangi birim altındadır; (Birden fazla birim de olabilir)
İç denetim birimi Risk yönetimi birimi Stratejik yönetim Diğer……...

2. Eğer Holding'e bağlı bir işletme iseniz Risk Yönetim uygulamanız holding'e bağlı mı yoksa ana şirket faaliyeti olarak mı yürütülmektedir?
Holding'e bağlı Ana şirket faaliyeti

3. Eğer bir risk yönetimi faaliyetiniz veya bu alanda bir planınız var ise bu hangi aşamadadır?

Tamamen yerleşik durumda,
Kısmen yerleşik durumda,
Yerleştirmek için planlanıyor,
Araştırılıyor, fakat henüz karar verilmiş durumda değil,
Yerleştirme planı yok

4. Risk yönetim uygulamasına ne kadar süre önce başladınız?

Üç yıl+	□	Bir yıl	□
Üç yıl	□	Bir yıldan az	□
İki yıl	□		

5. Hangi sebep(ler) veya ihtiyaç(lar)dan dolayı, risk yönetimi faaliyetine geçilmiştir ?

- Yasal zorunluluklar
- Daha etkin iç denetim ve kontrol ihtiyacı
- Performans eksikliği ile operasyonların verimliliğinin ve sürekliliğinin sağlanması
- Rekabet baskıları
- Artan kriz frekansı ile uygun bir kriz yönetimi ile krizlerin atlatılması
- Kurumun stratejisini etkileyebilecek potansiyel olayların belirlenmesi, yönetilmesi ve kurumun hedeflerine ulaşılmasının sağlanması ihtiyacı
- Finansal risklere karşı korunma ve finansal değişikliklerden faydalanma ihtiyacı
- Diğer …….

6. İç denetim ve risk yönetimi fonksiyonlarını yürütmekte olan birimlerin eleman sayıları ?

1–2 □, 3–5 □, 6–10 □, 11+ □

7. Risk yönetimi ve iç denetim çalışanlarının bilgi ve becerilerini artırmaya yönelik yapılan eğitimler veya planları var mı?

VAR YOK

8. Risk raporlama sisteminiz var mı, var ise nere(ler)e raporlama yapılmaktadır?

VAR		YOK	
Üst yönetim	□	Yönetim kurulu	□
Paydaşlar	□	Tüm şirket	□
Yasal ve		Diğer	□
Düzenleyici kurumlar	□	(Lütfen Belirtiniz)	

9. İşletmeniz belirlediği ve bildirdiği bir risk yönetim tüzüğü (Risk Yönetiminin amaçlarını ve taahhütlerini belirleyen resmi doküman) var mıdır?

EVET HAYIR

Var ise; bu tüzüğünüz şirketin tüm çalışanlarına bildirilmiş midir ?

EVET HAYIR

10. Risk Yönetim faaliyetleri kapsamında, aşağıda belirlenen faaliyetlerin hangileri, şirketin uygulamalarına yerleşmiş, halen yerleştirme devam etmekte ve gelecek için planlanmaktadır?
(Tamamen yerleşmiş (T), Yerleştirme devam etmekte(Y), gelecek için planlanmış(P) işaretlemesi ile belirtebilirsiniz.)

Risk yönetim prosesini ve/veya fonksiyonunu organize etmek
Kurum çapında riskleri belirlemek
Kurum çapında riskleri değerlendirmek
Risk yönetim pratiklerini geliştirmek için tavsiye ve öneriler vermek
Risk finanslama çözümlerini belirlemek ve uygulamak
Kurum çapında riskleri karşılamak
Şirket içinde belirlenmiş risk yönetim politikası ve standartları ile uyumu doğrulama
Yasal zorunluluk amacı için iç denetim işlerine katkıda bulunmak
Bir risk yönetim raporlaması ve bilgi sistemi kurmak
Kurum çapında risklerin kontrol aktiviteleri
Kurum çapında risklerin takip edilmesi
Şirket içinde risk yönetimini enlemesine uzanan şekilde koordine etmek ve kurmak

11. İşletmenizde risklerin belirlenmesi ve ölçülmesi için aşağıdaki yöntemlerden hangilerini kullanıyorsunuz?

Temel performans göstergeleri □
Temel risk göstergeleri □
İç değerlendirme □
Risk haritaları (belirleme, tanımlama ve önceliklendirme) □

Sayısal yöntemler (VaR, Monte Carlo, vb.) □
Diğer (Lütfen belirtiniz)……..……

Eğer Risk Haritalandırma var ise, ne sıklıkta yapılmakta?

Yılda Bir		Haftada Bir	
Üç Ayda Bir		Daha Sık	
Ayda Bir		Sadece uygulamaya geçerken	

12. Hangi risk grubuna daha çok odaklanmaktasınız ? (Odaklanma sıranıza göre numaralandırabilirsiniz)
Finansal □ Stratejik □ Operasyonel □ Çevre □ Tümüne aynı □

13. Kurumsal risk yönetimi konusunda şirket genelinde hangi standartları uyguluyorsunuz?

Coso	□	Australian Standard (AS/NZS 4360)	□
EU 8. Direktifi	□	Risk management standard	□
Sarbanes-Oxley	□	The combined code on corporate governance	□
Basel II	□	OECD principles of corporate governance	□

14. Hedeflediğiniz risk yönetimi ile şuan uygulamakta olduğunuz risk yönetim arasında fark var mıdır ?

EVET HAYIR

15. Risk yönetimi, kurumun hedeflerine ulaşma derecesini, faaliyetlerini ve geçmiş performansını ne sıklıkta gözden geçirmektedir?"

Yılda Bir		Haftada Bir	
Üç Ayda Bir		Daha Sık	
Ayda Bir			

16. Risk yönetimi konusunda harici bir danışmanlık hizmeti almakta mısınız?

EVET HAYIR

Eğer iç denetim biriminiz var ise bundan sonraki soruları cevaplayınız, yok ise 24. soruya geçiniz.

17. İç denetim işlevinin sürdürülmesi ile görevli yönetim kurulu üyesinin aynı zamanda risk yönetiminden de sorumlumudur?

EVET HAYIR

18. İç denetim, gerçekleştirilen iş ve eylemlerin belirlenmiş strateji ve politikalara/mevzuata uygunluğunu denetlemek temidir?

EVET HAYIR

19. İç denetçi, işletmenin varlıklarının ve kaynaklarının etkin bir şekilde kullanılıp kullanılmadığını değerlendirmek temidir ?

EVET HAYIR

20. Bir dış denetçi (Pwc, Kpmg, Ernest&Young, Deloitte,vs…) ile çalışıyor musunuz?

EVET HAYIR

21. İç denetim ile ilgili üst düzey risk komitesinde yer alabilecek kişiler var mıdır?

VAR YOK

22. İç denetim etkinliğini ölçüyor musunuz?, Ölçüyorsanız nasıl?

- İç denetimlerin iç denetim raporuna uygun olarak tamamlanması
- İç denetim raporlarının ne kadar sürede hazırlandığı
- İç denetim Planı kapsamındaki denetimleri zamanında tamamlayabilme

23. Uygulamada iç denetimin hangi işlevleri ön plana çıkmaktadır? (En önemli görülen işlevi 1'den başlatmak üzere sıralayınız)

Danışmanlık		Uygunluk Denetim	
Güvence		İş/Süreç Geliştirme	
Finansal Denetimi		Faaliyet Denetimi	
Risk Yönetimi			

24. Risk yönetiminden veya iç denetimden sağladığınız faydalar nelerdir?

Değer yaratacak riskleri alma □
Stratejik hedeflere ulaşılma □
Yeni pazarlara girme □
Karlılığın artması □
Rekabet edebilme □
Yasal ve idari düzenlemeler □
Düzgün kurumsal yönetim prosedürleri oluşturma □
Paydaş/hissedarlara gerekli bilgileri aktarma □
Performans izleme □
Karar mekanizmalarının ve iletişim ağlarının netleşmesi □
Ar-Ge'yi etkin hale getirme □
Diğer (Lütfen belirtiniz)
……..…….

25. Risk yönetimini veya iç denetimi işletmenize yerleştirirken karşılaştığınız zorluklar ve engeller nelerdir?

Risk Yönetim sistemini kurma maliyeti □
Kurumsallaşma eksikliği □
Devlet politikalarındaki değişiklikler □
Rakiplerin davranışları □
Ekonomik koşullar □
Risk yönetimine işletme içinde karşı olanların varlığı □
Diğer (Lütfen belirtiniz)
……..…….

EK A.2

Çizelge A.1 : KRY ve İç denetim ile ilgili anketten alınan sonuçlar.

KURUMSAL RİSK YÖNETİMİ VE İÇ DENETİM ANKET SONUÇLARI				
Şirketi Ve Risk Yöneticisini Tanımlayıcı Bilgiler İçi Soru Ve Cevap Şıkları				
Soru 1	**Risk Yönetim Müdürü/Direktörü**	**İç Kontol&RY Müdürü/Direktörü**	**Hissedarlar Servisi Müdürü**	**Uzman Yardımcısı**
R. Y. Pozisyonu	✓✓	✓✓	✓	✓
Soru	**İşletme**	**Mühendis**	**Uluslarar. ilişk.**	**Diğer**
R.Y. Eğitim Durumu	✓✓✓	✓✓	✓	✓✓
Soru	**1-4 yıl**	**10-14 yıl**	**15-19 yıl**	**25+ yıl**
İşletmenin Yaşı		✓		✓✓✓✓✓✓✓✓✓
Soru	**50-100**	**150-200**	**250-500**	**500+**
İşl. İstihdam sayısı				✓✓✓✓✓✓✓✓
Kurumsal Risk Yönetimi İle İlgili Bilgiler İçin Soru Ve Cevap Şıkları				
Soru	**VAR**	**YOK**		
Risk Yönet. Faaliyet	✓✓✓✓✓✓	✓✓		
Soru	**Risk Yönetim B.**	**İç Denetim B.**	**Risk Y.&İç K.**	**Stratejik Y. B.**
R.Y yürüten birim	✓✓✓		✓✓	✓
Soru	**Holding'e bağlı**	**Merkeze Bağlı**	**Ana Şirket Faaliyeti**	
	✓✓✓	✓✓	✓	
Soru	**Tamam. yerleşik**	**Kısmen Yerleşik**	**Planlanıyor**	**Araştırılıyor**	**Planlanmıyor**
KRY Aşaması	✓✓✓✓	✓✓	-	✓	✓
Soru	**1yıl**	**2yıl**	**3yıl**	**3+yıl**
KRY uygulama süresi		✓✓✓	✓	✓✓
Soru (Hangi sebepler veya ihtiyaçlardan dolayı risk yönetim faaliyetine geçilmiştir?)				
Yasal zorunluluklar	✓✓	Daha etkin iç denetim ve kontrol ihtiyacı	✓	
Artan kriz frekansı ile uygun bir kriz yönetimi ile krizlerin atlatılması	✓	Finansal risklere karşı korunma ve finansal değişikliklerden faydalanma	✓	
Performans eksikliği ile operasyonların verimlilik ve süreklilik sağlanması	✓✓✓✓	Stratejileri etkileyebilecek potansiyel olay belirleme, yönetme ve hedeflere ulaşma	✓✓✓✓✓	
Soru	**1-2**	**3-5**	**6-10**	**11+**
R:Y. Çalışan Sayısı	✓✓	✓✓✓✓		
İç D. Çalışan Sayısı				✓✓✓✓✓
Soru	**VAR**	**YOK**		
Eğitim	✓✓✓✓✓✓			
Soru	**VAR**	**YOK**		
Raporlama	✓✓✓✓✓✓	✓✓		
Soru	**Üst Yönetim**	**Paydaşlar**	**Yönetim Kurulu**	**Yasal, Düz. Kuruluşlar**	**Diğer(Süreç Sahipleri)**
Rapor. Kime	✓✓✓✓	✓✓✓	✓✓✓	✓	✓✓
Soru	**VAR+Evet**	**YOK+Hayır**		
R.Y.Tüzüğü+Bildirim	✓✓✓✓	✓✓		
Soru	**Tamamen Yer.**	**Yerleşme devam**	**Planlanıyor**	**Cevapsız**
RY prosesini ve/veya fonk. organize etme	✓✓✓✓✓	✓		
Kurum çapında riskleri belirleme	✓✓✓✓	✓✓		
Kurum çapında riskleri değerlendirme	✓✓✓✓	✓✓		
RY pratik. Geliştirme	✓✓✓✓	✓✓		
Risk finans. Çözüm. belirleme ve uygulama	✓✓✓	✓	✓	✓
Kurum çapında riskleri karşılamak	✓✓✓✓	✓		✓
Şirket RY politikası ve standartları ile uyumu doğrulama	✓✓✓		✓	✓✓

Çizelge A.1 : KRY ve iç denetim ile ilgili anketten alınan sonuçlar (devam).

Yasal zor. için iç denetime katkı	✓✓	✓		✓	✓✓
RY raporlaması ve bilgi sistemi kurmak	✓✓✓	✓✓		✓	
Kurum çapında risk kontrol aktiviteleri	✓✓✓	✓		✓✓	
Kurum çapında riskler takip etme	✓✓✓	✓✓		✓	
Şirkette KRY'i enine koordinasyon	✓✓✓			✓	✓✓
Soru	**Per. Gös.(KPI)**	**Risk Gös. (KRI)**	**İç Değerleme**	**Risk Haritaları**	**Sayısal Yöntemler**
Risk belir. ve ölçme yönt.	✓✓✓✓✓	✓✓✓✓✓	✓✓✓✓	✓✓✓✓✓	✓✓✓
Soru	Yılda	Üç ayda	Ayda	Haftada	Uyg.a geçer.
Risk Harita. Sıklığı	✓✓✓		✓		✓✓
Soru	**Finansal**	**Stratejik**		**Operasyonel**	**Çevre**
Önem puanı	4-2-1-4-4-4-3=22	1-3-3-3-2-4-4=20		3-4-4-0-3-4-1=19	2-1-2-0-1-0-2=8
Soru	**COSO**	**SOX**		**AS/NZS 4360**	**R. M. Standard**
Uyg.Standartlar	✓✓✓	✓		✓	✓✓
Soru	**VAR**	**YOK**		**Cevapsız**	
Hedef yapı farkı	✓	✓✓✓✓		✓	
Soru	**Yılda bir**	**Üç ayda bir**		**Ayda bir**	**Haftada bir**
RY Şirket hedeflere ulaşma performansı	✓	✓✓✓		✓	
Soru	**EVET**	**HAYIR**			
Harici Danışmanlık	✓	✓✓✓✓✓✓			
İç Denetim/Kontrol İle İlgili Bilgiler İçin Sorular Ve Cevaplar					
Soru	**EVET**	**HAYIR**		**Cevapsız**	
İD RY'den sorumlu?	✓✓✓	✓✓✓		✓✓✓	
İşlerin strateji ve mevzuata uygunluğu	✓✓✓✓✓✓			✓	
Varlık/Kaynak Etkinliği	✓✓✓✓✓✓			✓	
Dış Denetçi	✓✓✓✓✓✓✓			✓	
Ü.Risk Komitesi	✓✓✓✓	✓		✓✓✓	
Soru	**İç Denetim Etkinlik Kriter**				
Rapora uygunluk	✓✓✓✓	Rapor süreleri	✓✓	Zaman. denetim	✓✓

Soru	**Danışma**	**Güvence**	**Finans.D**	**Risk Y.**	**Uygunluk**	**İş geliştir.**	**Faali.D**
İç D. İşlev. Önem sıra	6	7	2	5	1	4	3.

Soru	**Kurumsal Risk Yönetiminin Sağladığı Faydalar**		
Değer yaratacak riskleri alma	✓✓✓✓	Stratejik hedeflere ulaşma	✓✓✓✓✓✓
Yeni pazarlara girme	✓	Yasal ve idari düzenlemeler	✓✓✓
Rekabet edebilme	✓✓	Karlılığın artması	✓✓✓
Düzgün kurumsal yönetim prosedürleri oluşturma	✓✓✓✓✓✓	Karar mekanizmaları ve iletişim ağlarının netleşmesi	✓✓
Paydaş/hissedarlara bilgileri aktarma	✓✓✓✓	Ar-Ge'yi etkin hale getirme	
Performans izleme	✓✓✓✓✓✓		
Diğer	Süreç geliştirme/iyileştirme,Verimlilik, kaynak kullanımı, bilgi güvenliği, işlerin denetimi, İç denetimi yasa ve yönetmeliklere uydurma		
Soru	**KRY'nin Getirdiği Zorluk Ve Engeller**		
KRY sistem kurma maliyeti	✓✓	Kurumsallaşma Eksikliği	✓✓
Devlet politika değişiklikleri	✓	KRY'e işletmede karşı olanların varlığı	✓✓
Rakip davranışları		Ekonomik koşullar	✓
Diğer	KRY Türkiye'de yeni ; model yapı✓ ve bilgi eksikliği✓✓, insanların değişkenliğe tepkisi✓		

ÖZGEÇMİŞ

Ad Soyad: Şule GÜNEŞ

Doğum Yeri ve Tarihi: İstanbul, 14.04.1984

Adres: Ş.Şahinbey Cad. Bolelli Sitesi No: 118 D/18 Çekmeköy - İSTANBUL

Lisans Üniversite: Yıldız Teknik Üniversitesi, Endüstri Mühendisliği

Yayın Listesi: Yok