Süleyman Demirel Üniversitesi
Vizyoner Dergisi
Y.2012, C.4, S.7. s.30-46

Suleyman Demirel University
The Journal of Visionary
Y.2012, C.4, S.7. s.30-46

KURUMSAL RİSK YÖNETİMİ VE KURUMSAL RİSK YÖNETİM SÜRECİ

Özen AKÇAKANAT*

ÖZET

Bu çalışmanın amacı, kurumsal risk yönetiminin yapısını farklı boyutlarıyla birlikte incelemektir. Çalışmada ayrıca bu yapının işleyişi ve uygulama süreci de ortaya konularak bir değerlendirme yapılmıştır. Bu değerlendirme sonucunda, organizasyonların risk dolu ortamlarda daha etkin ve yüksek performans ile faaliyet gösterebilmesi için etkin bir kurumsal risk yönetiminin gerekli olduğu belirlenmiştir. Çünkü organizasyonlar, kurumsal risk yönetimi uygulamaları sayesinde kaynaklarını en verimli şekilde tahsis etme ve kullanma fırsatı elde etmektedir.

Anahtar Kelimeler: Kurumsal risk yönetimi, kurumsal risk yönetim süreci, risk değerlendirme

ENTERPRISE RISK MANAGEMENT and PROCESS OF ENTERPRISE RISK MANAGEMENT

ABSTRACT

The aim of this study is investigating the structure of enterprise risk management through different aspects. Besides, on evaluation has been made by putting forth the structure's mechanism and application process of enterprise risk management. As a result of this evaluation, it has been determined that organizations need an effective enterprise risk management for effective and high performance in risky environment conditions. Because organizations, get the opportunity to asign the resources in an efficient way by enterprise risk management practices.

Keywords: Enterprise risk management, process of enterprise risk management, risk assessing

1. GİRİŞ

Organizasyonlarda risk yönetiminin rolü konusunda son yıllarda çok büyük değişiklikler gözlemlenmiş ve risk yönetimi çok önemli hale gelmiştir. Günümüzde başarılı organizasyonlar belirsizlik ortamından kaçınma yollarını aramak gibi bir çaba yerine risklerden fırsatlar elde etmeye odaklanmaktadır. Bunun sonucu olarak da geleneksel bakış açısıyla uygulanan risk yönetimi mevcut koşullarda yetersiz kalmaktadır. Buradan hareketle organizasyonlar

* Dr., Süleyman Demirel Üniversitesi Strateji Geliştirme Daire Başkanlığı, ozenakcakanat@sdu.edu.tr

farklı risk türlerini de, operasyonel ve stratejik riskler gibi, dikkate almaya ve bunları aktif olarak yönetmeye başlamışlardır.

Bir organizasyon mevcut risklerini yönetirken birbirinden tamamen farklı olan iki tür yol izleyebilir. Birincisi mevcut risklerini birer birer ele alıp yönetmek; ikincisi ise tüm risklerini sistemin bir parçası olarak görüp, onları bir risk yönetimi programı çerçevesinde bütün olarak yönetmektir. İkinci yöntem genel olarak Kurumsal Risk Yönetimi olarak adlandırılır. Organizasyonların kurumsal risk yönetiminden beklenilen faydaları elde edebilmeleri iyi işleyen kurumsal risk yönetim yapısı ve etkin kurumsal risk yönetim uygulamaları ile mümkündür. Bu bağlamda bu çalışmada etkin bir kurumsal risk yönetim yapısı oluşturmak için gerekli olan süreçlere değinilmektedir.

2. KURUMSAL RİSK YÖNETİMİNİN ÇERÇEVESİ ve KAPSAMI

Kurumsal risk yönetimine ilişkin COSO 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" (COSO, 2004).

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, s. 34).

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, kredi, likidite, itibar, iş devamlılığı, güvenlik, gizlilik, sektör spesifik, rekabet 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 (Tekgül, 2007, s. 4).

Bütün kurumlar belirsizlikle karşı karşıyadır, yönetimin çabası ortak değerini artırmaya çalışırken kurum için ne kadar belirsizliğin alınmaya hazır olunduğunun kararını vermektir. Belirsizlik hem riski hem de fırsatı içermektedir (COSO, 2004). KRY'nin ortaya çıkış gerekçesi risklerin de ortaya çıkış gerekçesi olan kurumun başarmayı hedeflediği stratejileri ve amaçlarıdır. KRY'nin temel amacı, risklerin yönetilmesi sağlanarak kurum amaçlarına ulaşmak olarak ifade edilebilir (Sobel, 2005, s. 88).

3. KURUMSAL RİSK YÖNETİMİNİN FAYDALARI VE SINIRLILIKLARI

Organizasyonlar sürekli değişim, artan rekabet, ekonomik dalgalanmalar, yasal zorunluluklar, gelişen teknoloji, küreselleşme gibi faktörlerin yarattığı belirsizlikler ile mücadele etmek için etkin iş çözümlerine ihtiyaç duymaya başlamıştır. Bu etkin çözüm yollarından biri de kurumsal risk yönetiminin organizasyonun süreçlerine dahil edilmesidir. Bu faydaların elde edilmesi doğru KRY yapısının tesis edilmesi ve etkin KRY uygulamaları ile mümkündür (Seuamsothabandith, 2004, s. 4). Kurumsal risk yönetiminin faydaları 3 eksende toplanabilir; işletme performansının artırılması, risk yönetimi maliyetinin optimize edilmesi, rekabet avantajı sağlanması (COSO, 2004). Kurumsal risk yönetimi organizasyonun performansını artırarak;

- Değişikliklere hazır olma durumunu geliştirir.
- Operasyonel kayıpları azaltır
- Düzenlemelere uyum ve risklere cevap vermeyi mümkün kılar
- Performans hedefleri ile ilgili belirsizlikleri tahmin edilmesini sağlar
- Sistematik risk değerlendirme sürecine güveni sağlar

Kurumsal risk yönetimi risk yönetim maliyetini optimize ederek;

- Fazla ve gereksiz faaliyetleri ortadan kaldırır
- Risklere uygun verilen cevapları bir araya getirir
- Risk işlem maliyetini düzenler
- Riskin ne kadarının tolere edileceğini belirler

Kurumsal risk yönetimi rekabet avantajı sağlayarak;

- Organizasyonun iş planları ile risk yönetimini uyumlaştırır
- Risk değerlendirme sürecinin güvenilirliğini sağlar
- Organizasyondaki tüm risklerin yönetimini sağlar
- Sermaye ve kaynak tahsisini geliştirir
- Öz değerlendirmelere göre risk alımını yapılandırır
- Marka imajını ve ününü korur.

KRY uygulamasının yukarıda sayılan çok sayıda faydası olmasına rağmen, burada dile getirilmesi gereken sınırlılıklar bulunmaktadır. KRY çok iyi tasarlanmış ve yürütülmüş olsa da sistemin sınırlarından ötürü makul düzeyde güvence vermenin ötesine geçilemeyebilir. Kurumsal risk yönetiminin en büyük kısıtı çalışma alanı olan risklerin belirsizlik ortamının bir sonucu olmasıdır. Bilindiği gibi riskler, geleceğin belirsizliğinden kaynaklanmaktadır ve bu belirsizliği ortadan kaldırmanın imkânı yoktur. Sistemin önündeki bir diğer kısıtta; risklerin hızlı bir şekilde değişebilmesi bundan dolayı daha önceden tanımlanan olasılık ve etkilerin geçerliliğini kaybetmesidir (The Institute of Internal Auditors Research Foundation (IIARF), s. 134). KRY'nin etkinliği yanlış kararlar verebilen insanlarla sınırlıdır. Kararlar, kısıtlı zamanda, mevcut verilerle ve işin doğurduğu baskı altında alınabilmelidir. Bazı kararların ileri tarihte hedeflenen sonuçları vermediği anlaşılır ve bu durumda düzeltilmesi gerekir. iyi planlanmış KRY'de de sorunlar çıkabilir. Kurum çalışanları talimatları yanlış anlayabilir, karar verme hataları yapabilir yahut ilgisizlik, dikkatsizlik ve yorgunluktan hatalar yapabilirler (Chapman, 2003, s. 33). KRY'de önemli bir kısıt da yönetimin KRY'ye gereken desteği vermemiş veya yetersiz vermiş olmasıdır.

4. KURUMSAL RİSK YÖNETİMİ SÜRECİ

Risk, organizasyonu bütünüyle etkileyebilecek olan faaliyetler ve mali kayıpla, etik olmayan davranışlar, güvenilirliğin sağlanamaması ve yasal gerekler ile çalışma politika ve prosedürlerine uygun olmama gibi bir olay ya da faaliyetin organizasyonu olumsuz yönde etkilemesidir. Başka bir ifade ile risk organizasyonun amaçlarına ulaşabilmesi veya belirlediği stratejileri başarılı bir şekilde uygulamasını engelleyen olay ve davranışlardır (Demirbaş, 2005, s. 177). Organizasyonun amaçlarını gerçekleştirebilmesi ve doğru kararlar alabilmesi için, öncellikli olarak karşılaştığı ve karşılaşması muhtemel riskleri tanımlaması, daha sonra bu riskleri değerlendirip analiz etmesi ve son olarak da bu riskleri yönetmesi gerekir (Ionescu, 2007, s. 131). Risklere uygun kontrol faaliyetlerinin belirlenmesi, bilgi ve iletişim ile izleme kurumsal risk yönetim sürecinin son adımlarını oluşturur.

4.1. Risklerin Tanımlanması ve Denetim Riski

Yukarıdaki tanımlarda da belirtildiği gibi risk, organizasyonun amaçlarına ulaşmasında ortaya çıkan engellerdir. Bu yüzden organizasyonlarda riski tanımlamadan önce, organizasyonun amaçları oluşturulmalı, daha sonra bu amaçlara ulaşmayı engelleyen riskler tanımlanmalıdır. Hem organizasyon düzeyinde hem de birimler düzeyinde açık, anlaşılır ve tutarlı amaçların oluşturulması risklerin tanımlanıp, değerlendirilmesi için ön şarttır (Dinapoli, 2009, s. 12-13).

Organizasyonun amaçları belirlendikten sonra, riskleri tanımlamak için organizasyon niteliksel ve niceliksel yöntemler kullanmalı ve bağıl risk dağılım planlarının ne olduğuna karar vermelidir. Riskler tanımlanırken risklerin tanımlanmasının nasıl yapılacağı, risklerin nasıl dağıtılacağı gibi konular ilgili çalışanlarla tartışılmalıdır. Burada da organizasyonun hem

kurumsal, hem de faaliyetler düzeyinde dışsal ve içsel faktörlerinden kaynaklanan riskleri tanımlayacak mekanizmaları kurması önemlidir. Dışsal faktörlerden kaynaklanan riskleri tanımlarken organizasyon şunları göz önünde bulundurmalıdır: Teknolojik gelişmelerden kaynaklanan riskler, yeni yasa veya düzenlemelerden kaynaklanan riskler, doğal afetler sonucu ortaya çıkabilecek riskler, politik, ekonomik değişikliklerden ortaya çıkabilecek riskler ve tedarikçilere ilişkin riskler. İçsel faktörlerden kaynaklanan riskleri tanımlarken ise şunlar göz önünde bulundurmalıdır: organizasyonun faaliyetlerinin veya çalışanlarının azaltılması sonucu ortaya çıkabilecek riskler, bilgi sistemlerinin ve yedeklemelerin uygulanmasına ilişkin bozulmaların ortaya çıkarttığı riskler, çalışanların işe yönelik becerilerinin eksikliğine ilişkin riskler, yönetimin değişmesinden kaynaklanabilecek riskler, yetkisiz kişilerin varlık ve kaynaklara erişiminden doğabilecek riskler, yeni program veya hizmetlerin uygulanmasından oluşabilecek riskler, yeni muhasebe ilkelerinin kabulü ya da değişiminden kaynaklanabilecek riskler (GAO, 2001, 23-25).

Organizasyon riskleri tanımlarken, denetimin değerlendirmelerine ilişkin denetim riskini de göz önünde bulundurmalıdır. Denetim riski, gerek iç denetçinin gerekse dış denetçinin, hem finansal kontrollerin hem de idari denetime ilişkin kontrollerin yanlış olduğu halde bilmeyerek doğru ve güvenilir olduğu hakkında olumlu görüş bildirmesidir. İç denetim, esas itibariyle, oluşturulan iç kontrol sisteminin amaçlandığı gibi çalışıp çalışmadığını inceleyen bu yönde üst yönetime rapor veren bir birimdir. İç denetimde de iç kontrol sistemini değerlendirmesine ilişkin çeşitli riskler bulunmaktadır (Demirbaş, 2005, s. 177). Denetim riski, doğal (yapısal) risk, kontrol riski ve ortaya çıkaramama riskinin bir fonksiyonudur. Yani:

Denetim riski= doğal risk x kontrol riski x ortaya çıkaramama riski

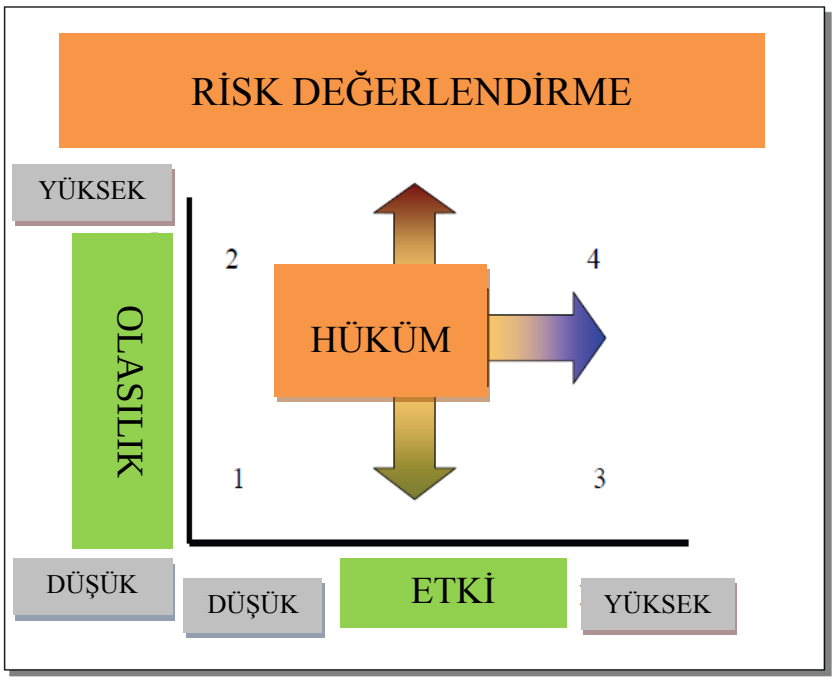
Doğal risk, iyi bir muhasebe ve iç kontrol sistemi olmadan doğabilecek risklerin toplamıdır. Kontrol riski ise, doğal risklerden iyi bir muhasebe ve iç kontrol sistemi sayesinde önlenenler çıktıktan sonra, hala kalan risklerdir. Ortaya çıkaramama riski de, kontrol sistemleri ile önlenmeyen ya da bulunamayan veya denetçinin de denetim teknikleri uygulayarak ortaya çıkarabileceği, ancak çıkaramadığı hata ve hilelerden doğan risktir (Kaval, 2005, s. 90-92).

4.2. Risklerin Değerlendirilmesi

Riskler tanımlandıktan sonra her bir riskin en iyi nasıl yönetileceğine karar verebilmek için risk değerlemesi yapılır. Risk değerlendirmesi, risklerin değerinin yani olası etkilerinin ve risklerin meydana gelme olasılığının hesaplanması, değerlendirilmesidir. Buradaki etki, riskin organizasyonun amaçlarını gerçekleştirme yeteneği üzerindeki önem derecesini ifade ederken; olasılık, riskin belirli bir zaman periyodu içinde gerçekleşme ihtimalini ifade etmektedir (Dinapoli, 2009, s. 13).

Şekil 1. riskleri değerlendirme konusunda makul bir yaklaşımı resmetmektedir. 1. bölge en düşük, 4. bölge en yüksek risk önceliğini temsil etmektedir. Yönetim, etkileri ve oluşma olasılıkları temelinde risk öncelikleri

oluşturabilmek için hüküm vermelidir. Riskler, en önemliden (yüksek etkili) ve gerçekleşme olasılığı en yüksek (yüksek olasılıklı) olandan (4. bölgede gösterildiği gibi), en az önemliye (düşük etkili) ve gerçekleşme olasılığı en az (düşük olasılıklı) olana (1. bölgede gösterildiği gibi) doğru mantıksal bir tarz izlenerek derecelendirilmelidir. Örneğin, bir program yöneticisinin iki adet nakit hesabı vardır. Biri ofis küçük masraf kasası diğeri ise program faaliyetinin harç ve cezaları için açılan hesaptır. Genel olarak küçük masraf kasası 1. veya 2. bölgede değerlendirilir. Cezalar ve harçların rakamsal büyüklüğünü, herkesin ulaşımına açık bir yerde saklandığını ve işlemlerinde altı aylık bir gecikme olduğunu gördüğünüzde bu 4. bölgeye uygun bir değerlendirme olabilir. Yöneticinin görevi 4. bölgedeki bu riski daha aşağıya çekmektir **(**Dinapoli, 2009, s. 14).



Şekil 1. Risk Değerlendirme

Kaynak: DINAPOLI, s. 13

Riskin etkisi ve meydana gelme olasılığı hesaplandıktan sonra, organizasyonun başa çıkması gereken risk kapasitesi belirlenir. Burada da kabul edilebilir ve istenmeyen organizasyon içi risklerin çeşit ve seviyelerine ilişkin üst yönetimin organizasyon çapındaki yöneticilere önderlik etmeleri önemlidir **(**Dinapoli, 2009, s. 14).

Kabul edilebilir risk ile kast edilen, organizasyonun ne kadar riski tolere edeceği ve organizasyonun ne kadar bir risk karşısında gerekli faaliyetleri yerine getireceğidir. Kabul edilebilir risk, organizasyonun faaliyetlerine, büyüklüğüne ve benzeri özelliklerine göre değişmektedir. Yani her organizasyon için kabul edilebilir risk düzeyi farklı olmaktadır (Intosai,

2004, s. 25). Organizasyon risklerin olası etkilerine ve gerçekleşme ihtimallerine göre risklerin çeşit ve seviyelerini belirledikten sonra bunları nasıl yöneteceğine karar verir.

4.3. Risklerin Yönetilmesi

Risklerin yönetilmesinde, yöneticiler belirli bir durumdaki riski kabullenmek, önlemek veya azaltmak ya da bu riskten tamamen kaçınmak arasında seçim yapabilmelidir. Örneğin, yetkisiz kişilerin elektronik dosyalara erişim hakkı kazanmaları ile ilgili riskin yönetimi ile ilgili karar verilirken yöneticiler aşağıdaki olasılıkları göz önünde bulundurmalıdırlar (Dinapoli, 2009, s. 14-15):

- Riski Kabullenmek - Kontrol Faaliyetlerini Gerçekleştirmemek: Yönetim yetkisiz erişim riskini bu tür bir erişimin sonuçlarının çok büyük olmaması sebebiyle kabullenebilir. Örneğin dosyaların içerdiği veriler hassas bilgi içermeyebilir. Yönetim ayrıca ilişkili kontrol faaliyetlerinin maliyetinin olumsuz olayın gerçekleşmesi sonucu görülecek zarardan daha fazla olması durumunda riski kabullenme yoluna gidebilir.
- Riski Önlemek veya Azaltmaya Çalışmak – Kontrol Faaliyetleri Gerçekleştirmek: Yönetim halihazırdaki yetkisiz erişim risk seviyesini dosyaların gizli ya da değerli bilgi içermesi sebebiyle kabullenmeyebilir. Bu sebeple yönetim yetkisiz erişim riskini önlemek ya da en azından kabul edilebilir bir seviyeye indirgemek amacıyla kontrol faaliyetleri oluşturur. Ancak, risk sadece kontrol faaliyetleri planlandığı gibi işlediği sürece azaltılacaktır.
- Riskten Kaçınma - Bu Fonksiyonu Artık Gerçekleştirmemek: Yönetim dosyalara yetkisiz erişim riskini tolere edemeyeceğini ya da bu erişimi yeterli seviyede kontrol edemeyeceğini değerlendirir. Örneğin: Bir dosya çok hassas veri içerebilir ya da erişim kontrolleri uygulanabilir olmayabilir. Bu durumda yönetim bu dosyaya erişimin etkilerinin çok riskli olabileceğine ya da erişim kontrolü faaliyetlerinin çok yüksek maliyetli olduğunu değerlendirebilir. Bu sebeple yönetim bu fonksiyonu yürütmemeye karar verebilir (yani, veriyi bulundurmamaya karar verebilir).

Riski önlerken ya da belirli bir seviyeye indirirken, yönetim riski idare edebilmek için en etkin ve verimli kontrol faaliyetlerini tanımlamaya yardımcı olacak risk değerlendirme bilgisini kullanmalıdır. Spesifik olarak yönetim risk değerlendirmede şu faktörleri göz önünde bulundurmalıdır (Dinapoli, 2009, s. 14-15):

- Riskin Nedeni Nedir? Yönetim riski azaltacak ya da önleyecek tüm olası kontrol faaliyetlerini tanımlamaya yardımcı olması amacıyla riskin varoluş sebebini göz önüne almalıdır.

- Kontrol Maliyeti ile Gerçekleşmesi İstenmeyen Olayın Maliyetinin Karşılaştırılması: Yönetim kontrol maliyeti ile olumsuz olayın kötü etkilerinin maliyetini karşılaştırmalı ve en düşük maliyetli seçeneği seçmelidir.
- Bu Riskin Önceliği Nedir? Yönetim, kaynakların risklerin azaltılması için kullanılan çeşitli kontrol faaliyetleri arasında nasıl paylaştırılması gerektiğine karar vermede yardımcı olması amacıyla öncelikli risk listesini kullanmalıdır. Öncelik seviyesine göre, kontrol faaliyeti için gerekli kaynak büyüklüğü planlanmalıdır.

Riskin değerlendirilip, yönetilmesi üstlenilecek uygun kontrol faaliyetlerinin seçilmesinde kilit bir rol oynar (Ionescu, 2007, s. 131).

4.4. Kontrol Faaliyetleri

Kontrol faaliyetleri, yönetim ve yönetim kurulu tarafından oluşturulan politika ve yöntemlerdir (Hallock, 2007, s. 8). Kontrol faaliyetleri, organizasyonun her bir fonksiyonu ve yönetim düzeyi için uygulanır, yani kontrol faaliyetleri organizasyon içerisinde tüm seviyelerde yer alır (Trenery, 1999, s. 18).

Kontrol faaliyetleri, organizasyonun plan, program ve hesap verilebilirliğinin ayrılmaz bir parçasıdır. Kontrol faaliyetlerinin etkinliğinden söz edebilmek için, amaca uygun olması, planlandığı gibi işlemesi, kapsamlı ve makul olması gerekir. Kontrol faaliyetleri, risk değerlendirme unsuru çerçevesinde belirlenen risklerin de izlenmesini sağlayacak şekilde düzenlemeli ve uygulanmalıdır. Bu şekilde düzenlenip uygulanan kontrol faaliyetleri risklerin ortadan kaldırılmasına aracılık eder (COSO, 2004, s. 49). Bir organizasyonun başarısını tehdit eden risklerle mücadele için birçok farklı kontrol faaliyeti kullanılabilir. Ancak çoğu kontrol faaliyeti önleyici ve tespit edici kontrol faaliyeti şeklinde ikiye ayrılabilir: (Dinapoli, 2009, s. 16)

- Önleyici Kontroller: Sorunlar ortaya çıkmadan önce, sorunların ortaya çıkmasını engelleyen kontrollerdir. Önleyici kontroller, istenmeyen olayın oluşumunu engellemek için tasarlanırlar. Bu kontrollerin gelişimi potansiyel problemlerin oluşmadan önce tahmin edilmesini ve bunları engelleme yöntemlerinin uygulanmasını içerir.
- Tespit Edici Kontroller: Sorunlar ortaya çıktıktan sonra bu sorunların ortaya çıkarılmasını sağlar. Tespit edici kontroller, gerçekleşen istenmeyen olayları tanımlamak ve yönetimi olay hakkında bilgilendirmek için tasarlanırlar. Bu kontroller, yönetimin düzeltici faaliyeti hızla gerçekleştirebilmesini sağlar.

Önleyici kontroller tespit edici kontrollere göre daha yoğundurlar. Önleyici ve tespit edici kontrollerin her ikisi de aynı kontrol hedefine ulaşmak için yapılırlar. Fakat önleyici kontrollerin geri beslemesi, tespit edici kontrollere göre daha hızlı olur. Tespit edici kontrollerin geri beslemesi daha ani ya da gecikmelidir. Örneğin gider döngüsü ele alındığında, nakit ödeme miktarlarının kontrolüne ilişkin (yetkisiz hiçbir harcamanın yapılmaması ve hiçbir gereksiz kaynak harcamasının yapılmaması için) kontrol faaliyetleri

uygulanacak olursa, yönetim spesifik olarak şu tip kontrolleri gerçekleştirebilir: (Christ vd., 2010, s. 1)

- Önleyici; çalışanların belirli bir miktarın üzerindeki harcamaları yapmaması için yetki limitleri uygulamak,
- Ani geri beslemeli tespit edici; belirli bir miktarın üzerinde harcamayı yapan çalışanın bilgisayarında alarm uyarısı oluşturulması,
- Gecikmeli geri beslemeli tespit edici; periyodik olarak, örneğin aylık, belirli miktar üzerindeki harcamaların rapor edilmesi.

Önleyici kontroller; görevlerin ayrımını, yetkilendirmeleri, onaylamaları ve doğrulamaları, kaynak ve kayıtlara erişimin sınırlandırmasını içerir (Evaluating Internal Controls, 2009, s. 7). Tespit edici kontroller ise; kayıtlar ile ilgili varlıklar arasında uyum sağlanmasını, performans göstergelerinin oluşturulması ve kontrolünü içerir. Bu sayılan kontrol faaliyetlerinden hiçbiri tek başına tüm risk yönetimi problemlerine çözüm sağlayamaz. Bazı durumlarda, çeşitli kontrol faaliyetleri kombinasyonu kullanılmalıdır bazı durumlarda ise bir kontrol faaliyeti bir diğerinin yerine konulabilir (Understanding Internal Controls, 2009, s. 10-11).

4.4.1. Görevlerin Ayrımı

Görevlerin ayrımı, bir faaliyetin yapılması aşamasında işi belirleyen, uygulayan, kayıtları tutan, varlıkları elinde bulunduranların ve onaylayanların aynı çalışanlar olmamasını ifade etmektedir. Yani, faaliyetlerin her aşaması farklı çalışanlarca yapılmalı ve sorumluluk aynı kişiye yüklenmemelidir. Örneğin, organizasyonda satın almada çalışan bir kişi aynı zamanda muhasebeden sorumlu olmamalıdır (COSO, 2004, s. 51).

Görevlerin ayrılmasında, görevler ve sorumlulukların, etkin bir kontrol ve denge sağlayacak şekilde farklı kişiler arasında sistematik olarak dağıtılması ve her işlemin operasyonel, idari ve mali yönü birbirinden bağımsız kişiler tarafından kontrol edilmesi önemlidir (INTOSAI, 2004, s. 29). Organizasyonda görevlerin ayrılması ile hata, kayıp, yolsuzluk gibi riskler azalır (GAO, 2001, s. 38).

4.4.2. Yetkilendirmeler, Onaylamalar ve Doğrulamalar

Yönetim, çalışanları sınırlandırılmış parametreler ile belirli işlemleri ve faaliyetleri yerine getirmek üzere yetkilendirir. Bu yetkilendirmeler, yazılı olarak ve açık bir şekilde yöneticilere ve çalışanlara iletilmelidir. Ayrıca, bu yetkilendirmeler özel koşulları ve hangi şartlar altında yetkilendirme yapılabileceğini de içermelidir. Yetkilendirme şartlarına uyulması çalışanların yönetim ve yasalar tarafından konulan sınırlar içinde kalarak direktiflere uygun olarak hareket etmesi anlamına gelmektedir (INTOSAI, 2004, s. 29). Yönetim, çalışanları yetkilendirdikten sonra, faaliyetler veya işlemlerin çalışanlar tarafından yerine getirilmesinden önce, yönetsel onaylara ve doğrulamalara ihtiyacı olan faaliyet veya işlemleri belirler. Yönetsel onaylar elle veya elektronik ortamda yapılabilir. Yönetsel

onayların ve doğrulamaların anlamı, faaliyet veya işlemlerin oluşturulan politika ve prosedürler ile uyumunun soruşturularak onaylanmasıdır **(**Understanding Internal Controls, 2009, s. 10).

4.4.3. Kaynak ve Kayıtlara Erişimin Sınırlandırılması

Kaynak ve kayıtlara erişim sadece yetkilendirilmiş çalışanlar ile sınırlandırılmalıdır. Kaynaklara erişimin sınırlandırılması, kaynakların yetkisiz kullanımının ve zarar görmesi riskinin azaltılmasını ve yönetim talimatlarının yerine getirilmesini sağlar (INTOSAI, 2004, s. 30).

Kaynak ve kayıtlara erişimin sınırlandırılmasına ilişkin çalışanların neleri yapıp neleri yapamayacaklarını bilmeleri gerekir. Burada da organizasyonun teşkilat şeması ve yazılı görev tanımları önem arz etmektedir (Carmichael ve Willingham, 1989, s. 164).

Varlıkların kullanma yetkisinin sınırlandırılmasına ilişkin kontrol faaliyetleri hem varlıkların fiziki kullanımını, hem de varlıkların kullanılması ve yönetilmesi yetkisini veren belgelerin hazırlanması ve işleme konulması ile varlıkların dolaylı kullanımını kapsar. Varlıkları kullanma yetkisi verilecek personelin sayısını ve uzmanlığını, varlıkların hatalı işlemlere ve yolsuzluklara elverişlilik derecesi belirler. Varlıkların korunması, uygun şekilde fiziki koruma amaçları ve donanımı ile korunmasını gerektirir. İşlemlerin, yönetimin devrettiği yetkilere dayalı olarak yürütülmesi ve yeterli düzeyde işbölümü yapılması, varlıkların korunmasıyla ilgili kontrol faaliyetleridir. Varlıkların fiziki korunmasına ilişkin kontrol faaliyetleri, sadece kilit, kasa, çit, güvenlik görevlisi bulundurma, yangın ve hırsızlığa karşı alarm sistemleri kurma gibi güvenlik araçlarını ve donanımlarını içermez; aynı zamanda muhasebe kayıtlarının ve kaynak belgelerin, hatta kullanılmamış önceden basılı belgelerin fiziki korunması, bu kayıtlara ve belgelere yetkili olmayan çalışanların erişiminin yasaklanması önlemlerini de içerir (Kepekçi, 1998, s. 73).

4.4.4. Kayıtlar ile İlgili Varlıklar Arasında Uyum Sağlanması

Varlıkların fiziksel olarak korunmasını sağlamak için, nakit ve diğer varlıkları, periyodik olarak ve fiziksel olarak saymak ve kayıtlar ile karşılaştırmak gerekir (COSO, 2004, s. 50). Burada önemli olan, işlem ve faaliyetlerin doğru olarak ve zamanında kayıt altına alınması ve güncellenmesidir. İşlemlerin ve faaliyetlerin, kontrol ve karar alma sürecindeki işlevini yerine getirebilmesi için anında ve doğru olarak kayıt altına alınması gerekir. Yasalara ve organizasyonun politika ve prosedürlerine uygun ve zamanında hazırlanan ve kaydedilen işlemler, hem kayıpları en aza indirir hem de hata yapılması durumunda hatanın tespit edilmesini kolaylaştırır (GAO, 2001, s. 39-40).

Hata ve yolsuzluklardan kolay etkilenen varlıklar bakımından karşılaştırma işlemi, varlıkların korunmasından ve kaydedilmesinden sorumlu olmayan çalışanlar tarafından yapılmalıdır. Varlıkların korunması ve finansal raporlara temel oluşturan kayıtların güvenilirliğine ulaşılması açısından bu karşılaştırmaların sıklık derecesi varlığın niteliğine, tutarına ve

karşılaştırma yapmanın maliyetine bağlıdır. Hesap ve tutarların doğruluğuna çeşitli kontrol usul ve yöntemleriyle ulaşılır. Çift taraflı kayıt yöntemi ve tahakkuk esaslı kayıt yöntemi bu kontrol yöntemlerindendir (Kepekçi, 1998, s. 43-44).

4.4.5. Performans Göstergelerinin Oluşturulması ve Kontrolü

Performans göstergeleri, organizasyonun amaç ve hedeflerine ulaşıp ulaşmadığını, ya da ne kadar ulaşıldığını ölçmek ve değerlendirmek için kullanılan ve sayısal olarak ifade edilen araçlardır (Bullen, 2010). Performans göstergeleri, farklı veri grupları arasındaki ilişkileri (faaliyet veya finansal) analiz etmek, farklılıkları araştırmak ve düzeltici işlemlerin yapılmasını sağlamak için araç vazifesi görür (Yılancı, 2006, s. 68). Bu yüzden organizasyonlarda, bireysel düzeyde, faaliyetler düzeyinde ve organizasyonun tamamı düzeyinde performans göstergeleri ve ölçümleri oluşturulmalıdır. Oluşturulan performans göstergelerinin doğruluğu ve güvenilirliği periyodik olarak gözden geçirilmelidir (GAO, 2001, s. 37).

4. 5. Bilgi ve İletişim

Organizasyonun riskleri hakkındaki bilgiler organizasyonda yukarıdan aşağıya doğru ve karşılıklı olarak iletilebilmelidir (Understanding Internal Controls, 2009, s. 17). Organizasyonların riskleri değerlendirilirken bilgi ve iletişime ilişkin şu sorular sorulmalıdır (Internal Control Guidance for Directors on the Combined Code, 1998, s. 14):

- Yönetim, karar vermek ve organizasyonu değerlendirmek için gereken iş hedefleri ve ilgili risklere ilişkin bilgileri içeren ilişkili ve güvenilir raporları zamanında alıyor mu? Bu raporlar müşteri tatmini ve çalışan davranışları gibi konulardaki nitelikli bilgi ile birlikte değişim göstergeleri ve performans raporlarını içerebilir.
- Hedefler ve ilişkili riskler değiştikçe ya da raporlama eksiklikleri tanımlandıkça bilgi ihtiyaçları ve ilişkili bilgi sistemleri yeniden değerlendirilmekte midir?
- Periyodik raporlama süreleri, altı aylık ve yıllık raporlama da dahil olmak üzere organizasyonun pozisyon ve beklentilerinin dengeli ve anlaşılabilir bir hesabını ortaya çıkarmak için etkin midir?
- Çalışanların ve diğer paydaşların şüpheli kanun dışı faaliyetleri ya da diğer düzensizlikleri bildirmesi için oluşturulmuş iletişim kanalları var mıdır?

4.5.1. Bilgi

Organizasyonların faaliyetlerini belirleyebilmek ve risklerini kontrol edebilmek için, hem içsel ve dışsal hem de finansal ve finansal olmayan, tutarlı, güvenilir ve doğru bilgiye ihtiyacı vardır. Bilgi, görev ve sorumluluklarını etkin ve etkili bir şekilde yerine getirmek için bilgiye ihtiyaç duyan organizasyonun tüm çalışanları ve yönetimi ile ilgilidir (GAO, 2001, s.

66). Güvenilir ve faydalı bilgi için ön koşul, işlemlerin ve olayların uygun bir şekilde sınıflandırılması ve kaydedilmesidir. İşlemler ve olaylar ortaya çıktıkları anda kaydedilirlerse, karar verenler ve operasyonları yönetenler için değerli ve tutarlı bilgiler sağlanmış olur. Yönetimin doğru kararlar verebilme yeteneği bilginin kalitesinden etkilenir (INTOSAI, 2004, s. 37-38).

Kaliteli bilgiler; (GAO, 2001, s. 62):

- Uygun (bilgi ihtiyaç olunan yerde mi?),
- Zamanlı (ihtiyaç olduğu zamanda elde mi?),
- Güncel (en son elde edilme zamanı ne?),
- Doğru (bilgi doğru mu?),
- Erişilebilir (konuyla ilgili kişiler tarafından kolayca elde edilebilir mi?) olmalıdır.

Organizasyonlardaki bilgi akışının kaynağı bilgi sistemleridir. Bilgi sistemi, muhasebe sistemini de kapsayan finansal raporlama amaçlarıyla ilgili kontrollerden ve belirlenmiş kayıtlardan oluşur. Kayıtlar; işletmenin varlıkları, borçları ve sermayesi ile ilgili sorumlulukların sürdürülmesi ve işlemlerin kaydedilmesi, sınıflandırılması ve özetlenmesinden oluşur. Sistemin ürettiği bilginin niteliği, güvenilir finansal raporların hazırlanmasına ve işletme varlıklarının kontrolüne ilişkin yönetimin alacağı kararlarda etkili olur (Uzay, 1999, s. 94).

4.5.2. İletişim

İletişim, bilgiden ayrı düşünülemez. İletişim, organizasyon ve çalışanlar arasında kararları destekleyen ve faaliyetleri koordine eden, faydalı bilgilerin değiş tokuşudur. Organizasyondaki iletişim sözel, yazılı veya elektronik olabilir. Sözel iletişim günlük faaliyetler için yeterli olabilirken, yine de bilgileri belgelere dayandırmak en iyisidir. Bu daha kalıcı kayıtlar sağlar ve çalışanlar ile yöneticilerin bilgileri gözden geçirmesini mümkün kılar (Dinapoli, 2009, s. 11).

Organizasyondaki tüm çalışanların bilgilendirilmesini sağlamak ve farklı birimlerin faaliyetlerinin koordinasyonu için bilgi tüm yönlere doğru iletilebilir olmalıdır. İyi bir iletişim sistemi organizasyondaki risklerin ortaya çıkarılması ve önlenmesi için önemlidir. İletişim sistemi faydalı bilgilerin tanımlanması, kayıt altına alınması ve değiş tokuşu için gerekli yöntemlerin oluşturulmasını içerir. Bu bağlamda yönetim (Dinapoli, 2009, s. 11);

- Zamanlı bilgi sağlayan,
- Bireysel ihtiyaçlar için adapte edilebilen,
- Çalışanları sorumluluk ve görevleri ile ilgili bilgilendiren,
- Önemli konuların raporlanmasını mümkün kılan,
- Çalışanlara organizasyonun gelişimi için öneride bulunmalarını sağlayan,
- Tüm çalışanların sorumluluklarını etkili bir şekilde yerine getirmeleri için gerekli olan bilgiyi sağlayan,
- Dış gruplar ile iletişimi sağlayan ve taşıyan,

- Üst yönetimin iç kontrol sorumluluklarının önemini ve sorumlulukların ciddiye alınmasına ilişkin mesajını taşıyan iletişim kanalları oluşturmalıdır.

Organizasyonlar, iç iletişim kadar müşteriler, tedarikçiler ve diğerlerinden oluşan dış paydaşlarıyla da uygun iletişim kanalları oluşturmalıdır. Bu iletişim kanalı halkla ilişkiler ile sınırlı kalmamalıdır. İç iletişim kanallarında olduğu gibi dış iletişimde de bilgi tüm yönlere doğru iletilebilir olmalıdır. Organizasyon dışına sağlanan bilgi organizasyon dışından olan kişilerin ihtiyaçlarını karşılayacak nitelikte olmalı ve bu kişilerin organizasyonu ve organizasyonun karşılaştığı sorunları daha iyi anlamalarını sağlamalıdır (COSO, 2004, s. 65).

4.6. İzleme

İzleme, organizasyonun performans kalitesinin değerlendirilmesidir (GAO, 2001, s. 57). Başka bir ifade ile izleme, organizasyonun belirli bir zaman aralığındaki performansının kalitesini değerlendirmek ve kontrollerin etkinliğini görebilmek için organizasyonun faaliyetlerinin ve işlemlerinin değerlendirilmesidir (Dinapoli, 2009, s. 22).

Organizasyonun izleme faaliyetini hangi sıklıkla yapacağı düşünüldüğünde, hem devam eden izleme faaliyetleri hem de bağımsız (ayrı) izleme faaliyetleri ile organizasyonların değerlendirilmesi söz konusudur. Yani izleme, devam eden izleme eylemlerini ve bağımsız (ayrı) değerlendirmeleri kapsar (GAO, 2001, s. 57).

Devam eden izleme faaliyeti, faaliyetlerin normal akışında organizasyonun etkinliğini değerlendirmeye hizmet eder. Doğrulamalar, kayıtlarla eldeki varlıkların karşılaştırılması, bilgisayar programlarıyla yürütülen kontrol yöntemleri, hesap bakiyelerindeki değişmelerin toplamlarının yönetim tarafından incelenmesi, bilgisayar raporlarının bunların kullanıcıları tarafından gözden geçirilmesi, devam eden izlemeye örnek olarak verilebilir (Doyrangöl, 2002, s. 34). Bağımsız izleme faaliyetleri, belli zamanlarda kontrollerin etkinliğine odaklanan yönetim tarafından yapılan kontrol öz değerlendirmeleri, iç denetçiler, dış denetçiler veya danışmanlık firmaları tarafından yapılan izleme faaliyetlerini kapsar (Understanding Internal Controls, 2009, s. 17).

4.6.1. Kontrol Öz Değerlendirme

Kontrol öz değerlendirme, devam eden izlemelerin verimliliğini sağlayan bağımsız değerlendirme faaliyetidir. Kontrol öz değerlendirme organizasyonun gerek bölüm bazında gerekse bütünsel olarak kendi kendini değerlendirmesidir (Evaluating Internal Controls, 2009, s. 14). Başka bir tanımla, kontrol öz değerlendirme, bölüm yöneticilerinin ve bölüm çalışanlarının oluşturduğu ve bölüm amaçlarına ulaşmak ve bu amaçlara ulaşma aşamasında karşılaşabilecekleri riskleri yönetmek amacıyla kullandıkları bir değerlendirme sürecidir. Amaç, tüm organizasyon

amaçlarının gerçekleştirildiği konusunda güven yaratmaktır (Keskin, 2006, s. 24-25).

4.6.2. İç Denetim

İç denetim, risk yönetim sisteminin amaçlandığı gibi çalışıp çalışmadığını inceleyen ve bu yönde üst yönetime rapor veren bir birimdir. İç denetimin amacı, sistemin üst yönetimin kararlarını gösteren yönetmeliklere ve yazılı emirlere ne derece uyulduğunu tespit etmek ve olumsuz gelişmeleri raporlamaktır (Kaval, 2005, s. 132).

İç denetçiler organizasyonun kontrol yapısının izlenmesinde önemli bir rol oynarlar. İç denetçiler organizasyonun kontrol yapısını değerlendirirken mali denetim, uygunluk denetimi, performans denetimi ve sistem denetimi uygulamalarını yaparlar. Mali denetim, mali raporlardaki verilerin, denetlenen birimin varlık ve yükümlülüklerinin gerçek değeriyle, finansman kaynaklarıyla, varlıklarının yönetimiyle ve tahsis edilen bütçe ödenekleriyle uyumlu olup olmadığının değerlendirilmesidir. Uygunluk denetimi, bir kurum ya da birimin mali işlemlerinin ve diğer faaliyetlerinin belirlenmiş yöntemlere, kurallara ve mevzuata uygun olup olmadığının incelenmesidir. Performans denetimi, kurum ya da birimin görevlerini yerine getirirken kullandığı fiziki, beşeri ve mali kaynakların ekonomiklik, etkinlik ve verimlilik derecelerinin değerlendirilmesidir. Sistem denetimi, denetlenen birimlerin mali yönetim usullerinin eksikliklerini tespit etme ve giderme konusunda etkili olup olmadığının değerlendirilmesidir (Çavuşoğlu, 2007, s. 4).

İç denetçilerin raporları kontrol zayıflıklarının belirlenmesinde ve düzeltme işlemlerinin gerçekleştirilmesinde önemli rol oynarlar (Yılancı, 2006, s. 84).

4.6.3. Dış Denetim

Dış denetim dış denetçiler tarafından yapılan denetimi ifade eder. Dış denetçiler, denetimini yaptıkları organizasyon ile ilişkisi olmayan yani organizasyondan bağımsız olan denetçilerdir. Dış denetçilerin kontrol değerlendirmesinin ve risk yönetiminin spesifik yönlerine ilişkin yardımcı bilgi ve erişime sahip olmalarından dolayı, organizasyonun kontrol sisteminin değerlendirilmesinde bağımsız izleme faaliyeti kapsamında dış denetçilere ihtiyaç duyulmaktadır (Internal Control Practical Guide, 1999, s. 41).

Dış denetimin, risk yönetim sisteminin yapısını anlaması, kontrol riskinin değerlendirilmesi için temel sağlar. Kontrol riski, denetim riskinin önemli bileşenlerinden biridir. Denetçiler, organizasyonun, kontrol yordamlarını gözlemleyerek, belgeleri inceleyerek, yönetimi ve çalışanları sorgulayarak kurumsal risk yönetim sistemini izlerler (Carmichael ve Willingham, 1989, s. 149-151).

5. SONUÇ

Artan rekabet ortamı, organizasyonları kendilerini yeniden yapılandırmak, örgütsel olarak yenilemek ve sermaye yapılarını güçlendirmek zorunda bırakmıştır. Bu kapsamda organizasyonlar finansal ve operasyonel risklerinin yanı sıra 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. Bunun sonucu olarak da kurumsal risk yönetimi, birçok organizasyon tarafından stratejik, finansal, operasyonel tüm risklerin belirlenmesi ve yönetilmesi, karşılaşılan ekonomik belirsizlikler karşısında dayanıklılık, sürdürülebilirlik ve esneklik elde edebilmek amacıyla artarak benimsenmektedir.

Bu çalışmada görülmektedir ki, kurumsal risk yönetimi risk dolu ortamlarda organizasyonların daha etkin ve yüksek performans ile çalışmasını sağlamaktadır. Kurumsal risk yönetimi uygulamaları sayesinde organizasyonlar kaynaklarını en verimli şekilde tahsis etme ve kullanma fırsatı elde etmektedir.

KAYNAKÇA

CARMICHAEL, D. ve WILLINGHAM, J. (1989), **Auditing Concepts and Methods A Guide to Current Auditing Theory and Practice**, McGraw-Hill Book Company, Fifth Edition.

CHAPMAN, C. (2003), "Bringing ERM into Focus" **Internal Auditor**.

CHRIST, M., EMETT, S., SUMMERS, S. ve WOOD, D., "The Effects of Preventive and Detective Controls on Employee Performance and Motivation, Working Paper Series, <http//ssrn.com/abstract=1489918>, (20.05.2010).

COSO, (2004), **Entity Risk Management – Integrated Framework.**

ÇAVUŞOĞLU, M. ve OSMAN, D. (2007), "İç Denetim", **Siyasal Vakfı Bülteni**, Sayı: 20 (Aralık).

DEMİRBAŞ, M. (2005), "İç Kontrol ve İç Denetim Faaliyetlerinin Kapsamında Meydana Gelen Değişimler", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Sayı: 7 (Bahar), s. 167-188.

DINAPOLI, T. (2007), **Standards for Internal Control in New York State Government**, <http://www.osc.state.ny.us>, (10.12.2009).

DOYRANGÖL, N. C. (2002), "İşletme Çevresindeki Olumsuz Gelişmeler Karşısında İç Denetimin Yeri ve Önemi", **Mali Çözüm Dergisi**, Sayı: 60 (Tem-Ağu-Eyl), s. 33-42.

Evaluating Internal Controls, Ernest & Young, Fourth in Series, <http://www.sarbanes-oxley.be/sarbanes-oxley_effectiveness.html>, (15.01.2009)

GAO (2001), **Internal Control Management and Evaluation Tool**, August.

HALLOCK, M. (2007), "Ethics & Internal Controls", **U. S. Business Review**, Volume: 8, Issue: 1, January, s. 7-8.

INTOSAI (2004), **Guidelines for Internal Control Standarts for the Public Sector**, Belgium, <http://intosai.connexcc-hosting.net/blueline/upload/1guicspubsece.pdf>, (15.01.2009).

IONESCU, L. (2007), "Internal Control, Human Resource Management and Risk Assessment", **Economics, Management and Financial Markets**, Volume: 2, Issue: 2, s. 129-136.

KAVAL, H. (2005), **Uluslararası Finansal Raporlama Standartları Uygulama Örnekleri İle Muhasebe Denetimi**, Gazi Kitabevi, Ankara.

KEPEKÇİ, C. (1998), **Bağımsız Denetim**, Siyasal Kitabevi, Ankara.

KESKİN, D. (2006), **İç Kontrol Sistemi Kontrol Öz Değerlendirme**, Beta Basım Yayım, İstanbul.

MCNALLY, S. (2007), "Control Self-Assessment: Everbody Pitching in with Internal Controls", **Pennsylvania CPA Journal**, Volume: 78, Issue: 3, s. 6-9.

Office of the Comptroller Commonwealth of Massachusetts, **Internal Control Guide for Managers,** , http://www.mass.gov/Aosc/docs/business_functions/bf_int_cntrls/icgsec1.pdf, (15.01.2009).

PAUL, S. (2005), **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA.

SEUAMSOTHABANDITH, S. (2004), **An Examination on Enterprise Risk Management**, Western Illinois University Press, USA.

TEKGÜL, E. (2007), **"**Kurumsal Risk Yönetimi ve Risk Zekası", **Referans Gazetesi**, Kasım.

The Institute of Chartered Accountants in England&Wales (1999), **Internal Control Guidance for Directors on the Combined Code**, September.

The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing**, https://na.theiia.org/iiarf/PublicDocuments/ResearchOpportunitiesinInternalAuditing.pdf, (15.01.2009).

The KPMG Review (1999), **Internal Control Practical Guide**, October.

THORNTON, G. **(**2003), "An ERM Framework: Developing Effective Risk Management", **Corporate Governor Series**.

TRENERY, A. (1999), **Principles of Internal Control**, University of New South Wales Press, Australia.

Understanding Internal Controls, A References Guide for Managing University Business Practices, <http://www.ucop.edu/ctlacct/under-ic.pdf>, (15.01.2009)

UZAY, Ş. (1999), **İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Dış Denetim Karar Sürecindeki Yeri ve Türkiye'deki Denetim Firmalarına Yönelik Bir Araştırma**, Sermaye Piyasası Kurulu Yayınları, No 132, Ankara.

YILANCI, M. (2006), **İç Denetim Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma**, Nobel Yayın Dağıtım, Ankara, Eylül.