Marmara Üniversitesi Öneri Dergisi • Cilt 12, Sayı 46, Temmuz 2016, ISSN 1300-0845, ss. 155-177
DOI: 10.14783/od.v12i46.1000010009

COSO İÇ KONTROL MODELİNDE RİSK DEĞERLENDİRME FAALİYETLERİ

Hasan TÜREDİ*
Ahmet Oğuz KOBAN**

Öz

İşletmeler belirli amaçlarla kurulmakta ve hedeflerini gerçekleştirecekleri faaliyetleri sürdürürken sürekli risk ve belirsizliklerle karşılaşmaktadırlar. İşletmelerin sonsuza dek yaşayacakları varsayılmaktadır. İşletmenin sürekliliği olarak adlandırılan bu kavram, kurumun değişen dışsal koşullara sürekli uyum sağlayabilmesini, hayatta kalmasını sağlayacak özel yetkinlikler geliştirmesini ve maruz kaldığı riskleri değerlendirip yönetebilmesini gerektirmektedir. COSO iç kontrol çerçevesi, kurumların sürdürülebilir başarıyı yakalayabilmesinin ön koşullarından biri olan iç kontrol yapısının kurulması, yönetilmesi ve gözetilip geliştirilmesini amaçlayan ve uygulamaya yönelik önerileri bulunan uluslararası iş dünyasında geniş kabul görmüş bir yaklaşımdır. COSO iç kontrol yapısının beş ana unsurundan biri olan risklerin değerlendirilmesi, işletmelerin maruz kaldığı riskleri tanımlayıp değerlendirdikten sonra önem derecesini de dikkate alarak en doğru yöntemlerle yönetmesini kapsamaktadır. Bu çalışmada COSO iç kontrol yapısı ve unsurları tanıtılmış ve risklerin değerlendirilmesi kavramı, reel sektörden örnekler verilerek irdelenmiştir.

Anahtar Kelimeler: COSO, İç kontrol, Risk Değerlendirme.

RISK ASSESSMENT ACTIVITIES IN COSO INTERNAL CONTROL MODEL

Abstract

The companies pursue their goals and operate their activities in an environment full of risks and uncertainties. One of the major principles in accounting is that the companies to conti-

* İstanbul Ticaret Üniversitesi, İşletme Fakültesi, Muhasebe ve Denetim Bölümü, Öğretim Üyesi, Prof.Dr.
** İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Programı, Doktora Öğrencisi.

nue indefinitely, which is called "the going concern assumption". Any company, surrounded by many risks must adapt to the rapidly changing conditions of the business environment, realize and manage those risks and build some core competencies to continue as a going concern. COSO internal control, having practical application tools for companies is one of the generally accepted frameworks that aims enabling the companies to build, manage and develop an internal control structure as a tool to reach sustainable success. One of the five COSO components is "risk assessment" covering the recognition and assessment of the potential risks that the company faces and manage those risk considering their materiality. This study aims to explain the COSO internal control model with its five components as well as stressing the assessment of risks component supported by some examples.

Keywords: COSO, Internal controls, Risk Assessment.

I. GİRİŞ

İç kontrol, işletmenin tüm faaliyetlerini içeren temel yönetim kavramlarından biridir. Bir işletmenin etkin bir iç kontrol yapısına sahip olmasının ne anlama geldiği ise uzun yıllar yeterince net olmayan, tartışmalı bir konu olarak kalmıştır. İç kontrolün net olarak tanımlanması, kapsamının ve unsurlarının tutarlı bir şekilde ortaya konması amacıyla ABD'de beş bağımsız meslek kuruluşu tarafından Committe of Sponsoring Organizations (COSO) 1990'larda oluşturuldu. 1992 yılında da etkin bir iç kontrol yapısının özellikleri ve kapsamını tanımlayan COSO İç Kontrol Yapısı (COSO Internal Control Framework) yayınlandı. Önceleri uygulanması zorunlu olmayan bu yapı, zamanla Sarbanex-Oxley (SOx) yasaları kapsamında bağımsız denetçi raporunun uyması gereken kurallar bütününe temel oluşturdu. İş dünyasının giderek daha fazla küreselleşmesi, bilgi teknolojileri ve iletişimde yaşanan hızlı gelişmeler COSO'nun Mayıs 2013'te bu gelişmelere ayak uyduracak şekilde yeniden düzenlenmesi ile sonuçlandı.

COSO modelinde iç kontrolün unsurlarından biri olan "Risklerin Değerlendirilmesi", işletmenin maruz kaldığı risklerin tespit edilip etkililiğine göre önceliklendirilmesi ve uygun karşılık verme yöntemlerine karar verilmesini içerir. Bir yandan işletmenin sürekliliğini sağlayabilmek için mevcut fırsatların farkına varması, diğer taraftan faaliyet sonuçlarını önemli ölçüde olumsuz yönde etkileyebilecek tehditlerin farkına vararak gereken önlemleri alması olarak da değerlendirilebilir. İşletmenin sürekliliği, işletmenin ortaklarının ömür süreleriyle sınırlı kalmaksızın faaliyetlerini sürdüreceğini öngörür [1].

Teknolojinin işletme faaliyetlerinin neredeyse tamamına nüfuz etmesi, uluslararası faaliyet hacminin giderek artması, iletişim kanallarındaki gelişmeler ve bilgiye erişim olanaklarının artışının sonucu olarak işletmelerin maruz kaldıkları riskler çeşitlenmiştir. Sundukları ürün ve hizmetleri çeşitlendirip karlı bir şekilde sürekli büyüme hedefine yönelik faaliyet gösteren işletmeler, bir yandan da bu hedeflerine ulaşmalarını engelleyebilecek tüm olaylarla, yani risklerle mücadele etmektedirler. Risk yönetimi kavramı geçmişte sadece bankalar ve sigorta

kuruluşlarının faaliyet alanına girerken, günümüzde hizmet ve üretim iş kollarında da tüm yöneticilerin gündemine girmiş, bu durum da beraberinde risk yönetiminin temelinde yer alan iç kontrol yapısı konusunun önemini artırmıştır. Etkin bir iç kontrol yapısı işletme varlıklarının olası hata ve hilelerden zarar görmesini engellerken, malî raporların zamanında ve doğru olarak düzenlenmesini, faaliyetlerin iktisadî ve verimli olarak yürütülmesini ve bunların yanı sıra yasal mevzuat ile iç yönergelere uyumu da sağlamaktadır.

COSO, 1990'larda yaşanan büyük ölçekli muhasebe ve malî raporlama hileleri sonrası muhasebe ve denetim alanında çalışmalar yapan bazı mesleki kuruluşların bir araya gelmesiyle oluşturulmuş bir yapıdır. Açılımı, "Committee of Sponsoring Organizations", yani "Sponsor Kurumlar Birliği" dir. Amerikan Malî Müşavirler Odası'nın da içinde bulunduğu bu birliğin amacı, iç kontrolun net olarak anlaşılmasını sağlanmak ve işletmelerde uygulanabilmesi için yol gösterici önerilerde bulunmaktır [2].

Bu çalışmada iç kontrol yapısının tanımı ve unsurları açıklandıktan sonra risklerin değerlendirilmesi faaliyetleri de detaylı olarak irdelenmiştir.

II. İÇ KONTROL YAPISI

II.1. İç Kontrol Yapısının Tanımı ve Amaçları

İç kontrol kavramı muhasebe ve bağımsız denetim ile birlikte gelişmiştir. Kıta Avrupası'nda iç kontrol, tanımlanmış işlemlerin geçmişe dönük olarak kontrol edilmesi olarak tanımlanmaktadır. Anglosakson geleneğinde ise iç kontrol, faaliyet sürecinin bütününün kontrol altında tutulmasını sağlayan bir yönetim mekanizmasıdır [3].

İç kontrol ile ilgili ilk kapsamlı araştırma 1949 yılında yapılmıştır. "Denetim Yordamları Komitesi"nin yayınladığı özel raporda iç kontrol şu şekilde tanımlanmıştır: "İç kontrol, örgütün planı ile işletmenin varlıklarını korumak, muhasebe bilgilerinin doğruluğunu ve güvenilirliğini araştırmak, faaliyetlerin verimliliğini arttırmak, saptanmış yönetim politikalarına bağlılığı özendirmek amacıyla kabul edilen ve uygulamaya konulan tüm önlem ve yöntemleri içerir" [4].

İç kontrol yapısı, yönetime hedef ve amaçlarını gerçekleştirebilmesi için makul güvence (reasonable assurance) veren politika ve yönergelerden oluşur. Bu politika ve yönergeler genellikle kontroller olarak adlandırılır ve bir araya geldiklerinde bütününe işletmenin iç kontrol yapısı denir [5].

Makul güvence, yüksek düzeyde bir güvencedir. Denetçinin hatalı malî tablolara dair uygun olmayan görüş bildirme riskini (denetim riskini) azaltmak için denetçinin yeterli ve uygun denetim kanıtını elde ederek denetim riskini kabul edilebilir seviyeye indirmesidir [6].

COSO tanımına göre de iç kontrol, işletme faaliyetlerinin etkinliği ve verimliliğinin, malî raporlamanın güvenilirliğinin, yasa ve mevzuata uyumun sağlanması için makul güvence ver-

mek üzere tasarlanan, kurumun yönetim kurulu, yönetimi ve çalışanları tarafından etkilenen bir süreçtir [2].

İç kontrol yapısının, işletmede aşağıdaki hususlar çerçevesinde makul bir güvence sağlamasına büyük etkisi vardır. Bu itibarla, bir işletmedeki tüm yöneticilerin etkin iç kontrol yapısı oluşturup bunun sürdürülebilirliğinin önemini kavramaları hayati önem taşımaktadır. Bunlar aşağıdaki gibidir [7]:

- Kanunlara, diğer düzenlemelere ve yönetimin belirlediği politikalara uyulması,

- Düzenli, etkin, verimli ve az maliyetli faaliyetleri özendirip planlanmış çıktıları gerçekleştirmesi,

- Hileye, israfa, kötü kullanım ve kötü yönetime karşı varlıkların korunması,

- Kurumun hedeflerine, kalite standardına uygun ürünler ve hizmetler sunulması,

- Güvenilir malî ve yönetim bilgileri oluşturulup bunun sürdürülmesi ve düzenli raporlar ile bu bilgilerin tarafsız biçimde ve zamanında açıklanması,

- Her türlü işletme kaynaklarının korunması.

Hile, belirli bir işletme, kişi veya grubun aleyhine olacak şekilde; şahsi çıkar sağlamak amacıyla ve kasti olarak yapılan yanıltıcı fiillerdir.

İç kontrol ile kurumal yönetimin de doğrudan ilişkisi bulunmaktadır. Kurumsal yönetim, işletmelerin her şart ve durum altında faaliyetlerini devam etmesini sağlamaya yönelik bir yönetsel politikalar bütünüdür [8]. Kurumsal yönetimin genel kabul görmüş adillik, şeffaflık, hesap verebilirlik ve sorumluluk ilkeleri de iç kontrol unsurlarıyla doğrudan ilgilidir.

II.2. COSO Modelinde İç Kontrol Yapısının Unsurları

Bir işletmede iç kontrol yapısının yeterli seviyede uygulanabilmesi ancak iç kontrol bileşenleri ile mümkündür. Bu bileşenler iç kontrol yapısı için bir çatı görevi gören COSO (The Committee of Sponsoring Organizations) tarafından ayrıntılı olarak ele alınmıştır. Beş adet bileşen şunlardır [2]:

a) Kontrol Ortamı

b) Risklerin Değerlendirmesi

c) Kontrol Faaliyetleri

d) Bilgi ve İletişim

e) İzleme.

Bu bileşenlerin her biri biribiriyle ilişki içindedir. Yenilenmiş COSO iç kontrol yapısı, Şekil 1'de görülebileceği üzere üç boyutlu bir küp şeklinde tasvir edilmiştir.

Birinci boyut iç kontrolün amaçları olup üç ana başlıkta incelenmektedir: "Faaliyetler", "Malî Raporlama" ve "Uygunluk". Küpün ikinci boyutunda iç kontrolün beş unsuru yer almaktadır. Küpün üçüncü boyutunda işletmenin teşkilat yapısı, yani işletmenin genel kurumsal yapısı, alt bölümleri, varsa iştirakleri ve ayrıntılı faaliyetleri yer almaktadır. Burada vurgulanmak istenen konu, işletme faaliyetleri için belirlenmiş olan kontrollerin, işletmenin bütünü için belirlenen kontrollerle uyumlu olmasının önemidir.

Şekil 1. COSO'nun Üç Boyutlu İç Kontrol Yapısı

Kaynak: [2].

COSO modelinin yukarıda sayılan beş unsuru özet olarak şu şekilde açıklanabilir:

II.2.1. Kontrol Ortamı

Kontrol ortamı, işletme yönetimi ve çalışanlarının iç kontrol yapısı ile ilgili davranış ve tavırları, yönetim ilkeleri, işletmenin örgütsel yapısı, yetki ve sorumlulukların dağıtılmasında izlenecek kural ve yöntemler ile personel politikalarından oluşmaktadır. Bu unsur, iç kontrol ortamını her yönüyle kapsamaktadır. Kontrol ortamının asıl kaynağını kurumun geçmişi, kurumsal kültür ve yönetim felsefesi oluşturmaktadır. Kurumdaki yönetim stili, yönetimin kontrol yöntemleri, personel politikaları, yönetim kurulu ve denetim komitesinin işlevi, yetki ve sorumlulukların dağılımı ve iç denetimin kurum içindeki rolü bu kapsam dahilindedir.

Kontrol ortamını oluşturan ilkeler şunlardır:

- Dürüstlük ve meslek ahlakı,
- Yönetim kurulunun iç kontrol faaliyetlerini gözetim sorumluluğu,
- Görev ve yetki dağılımlarının belirlenmesi,
- Yetkinlik taahhüdünün tesisi, çalışanların teşviki ve geliştirilmesinin tesisi
- Yetki ve sorumluluklar [9].

II.2.2. Risklerin Değerlendirilmesi

İşletmeler kendilerine tahsis edilen kaynakları amaç ve hedeflerine ulaşmak için kullanırlar. Bu kaynakların kullanımı amacıyla alınan kararlar, yürütülen faaliyet, süreç ve projeler beraberinde riskleri de getirir. Risk yönetimi, işletmelerin amaç ve hedeflerine ulaşmalarına yardımcı olan bir araçtır. Risk yönetimi, risk stratejisinin belirlenmesi, risklerin tespit edilmesi, değerlendirilmesi, risklere verilecek cevapların belirlenmesi, risklerin gözden geçirilmesi, izlenmesi ve raporlanması aşamalarını kapsar.

İşletmelerin sistemli bir şekilde incelemeler yaparak amaç ve hedeflerinin gerçekleştirilmesini engelleyebilecek iç ve dış riskleri tanımlayarak değerlendirmesi ve alınacak önlemleri belirlemesine risklerin belirlenmesi ve değerlendirilmesi denir [10].

Bu çalışmanın ana konusu olduğu için ileride ayrıntılı olarak açıklanmıştır.

II.2.3. Kontrol Faaliyetleri

Kontrol faaliyetleri, öngörülen bir riskin olasılık ve/veya etkisini azaltmayı ve böylece işletmenin amaç ve hedeflerine ulaşma şansını artırmayı amaçlayan eylemlerdir. Kontrol faaliyetlerinin belirlenmesi, risk değerlendirmesinin tamamlanmasına bağlıdır. Yönetim görevlerin ve hedeflerin gerçekleştirileceğine dair makul güvence elde etmek için, risk yönetimini esas almak suretiyle kontrol faaliyetlerini planlamalı, bunları düzenlemeli ve yönlendirmelidir. Kontrol faaliyetleri malî olan ve olmayan kontrolleri kapsamakta olup, işletmenin tüm faaliyetleri için bir bütün olarak tasarlanıp uygulanmalıdır [10].

II.2.4. Bilgi ve İletişim

Bilgi ve iletişim, diğer dört unsur arasındaki ilişkiyi bilgi paylaşımı ve iletişim yoluyla sağlar. İşletme genelinde bilgi akışını düzenleyerek kurumsal amaç ve hedeflere ulaşma yolunda bir araç olarak görülen iç kontrol yapısının işlerliği ve uygulanma kabiliyetinin artmasında önemli bir role sahiptir. İletişim, bilginin işletme içinde gerek yatay ve dikey olarak, gerekse

işletme dışında uygun araçlarla ilgili kişi, idare ve mercilere iletilmesini ve dönüşümünü ifade eder [10].

II.2.5. İzleme

İzleme, işletmenin amaç ve hedeflerine ulaşma konusunda iç kontrol yapısının beklenen katkıyı sağlayıp sağlamadığının, iç kontrol standartlarına uyum çerçevesinde değerlendirilmesi ve sistemin iyileştirmeye açık alanlarına yönelik eylemlerin belirlenmesidir. İzleme ile, işletmenin faaliyetlerinin amaç doğrultusunda, hedeflerle uyumlu olarak yürütülüp yürütülmediği, risk yönetimi esasları çerçevesinde gerekli kontrollerin öngörülüp öngörülmediği, söz konusu kontrollerin uygulanıp uygulanmadığı, iletişimin açık ve yeterli olup olmadığı gibi hususlar değerlendirilmektedir [10].

II.3. Türkiye'de İç Kontrol Düzenlemeleri

Türkiye'de halka açık şirketler, bankalar ve diğer işletmeler için iç kontrol kapsamında düzenlemeler bulunmaktadır. Ülkemizde iç kontrol yapısına yönelik ilk düzenleme 1996 yılında yayınlanan X,16 seri nolu "Sermaye Piyasasında Bağımsız Denetim Hakkında Tebliğ"dir. Daha sonra X,19 numaralı tebliğ ile SOx düzenlemelerinin etkisinin Sermaye Piyasası Kurulu (SPK) mevzuatına yansıtıldığı görülmektedir [11]. SPK düzenlemesinde iç konrol yapısının unsurları COSO modeline paralellik göstermektedir. Buna göre, iç kontrol çevresi, risk değerlendirme süreci, malî raporlama ve iletişim faaliyetleri, kontrol işlemleri ve kontrollerin gözetimi, iç kontrol yapısının unsurlarıdır.

SPK'nın 03.01.2014 tarihli Resmî Gazete'de yayınlanan II.17.1 sayılı Kurumsal Yönetim Tebliği'nin 4.1 maddesinde tanımlandığı üzere Yönetim Kurulu alacağı stratejik kararlarla şirketin risk, büyüme ve getiri dengesini en uygun düzeyde tutarak akılcı ve tedbirli risk yönetimi anlayışıyla şirketin öncelikli uzun vadeli çıkarlarını gözeterek şirketi idare ve temsil eder. Yönetim Kurulu ayrıca,

- şirketin uzun vadeli hedeflerini tanımlar,
- şirketin ihtiyaç duyacağı işgücü ile malî kaynakları belirler,
- yönetimin performansını denetler.

SPK'nın aynı tebliğinin 4.5 maddesinde "Riskin Erken Saptanması Komitesi" kurulması düzenlenmiştir. Bu komitenin görevleri de,

- şirketin varlığını, gelişmesini ve devamlılığını tehlikeye düşürebilecek risklerin erken teşhisi,
- tespit edilen risklerle ilgili gerekli önlemlerin alınması,
- riskin yönetilmesi amacıyla çalışmalar yapmak
- risk yönetim sistemlerini yılda en az bir kere gözden geçirmek olarak tanımlanmıştır [12].

Bankalar kanunu, iç kontrol yapısının mevzuata uygun şekilde tesis edilmesi, planlanması, etkin şekilde uygulanması ve malî raporlama sistemlerinin güvenilirliğinin sağlanması hususundaki sorumluluğu banka yönetim kuruluna vermiştir [13].Bankalar, maruz kaldıkları risklerin izlenmesi ve kontrolünün sağlanması için faaliyetlerinin kapsamı ve yapısıyla uyumlu, yeterli ve etkin bir iç kontrol sistemi kurmak ve işletmekle yükümlüdürler.

Bankalar faaliyetlerinin mevzuata, iç düzenlemelerine ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve raporlama siteminin etkin bir şekilde çalışarak raporları zamanında düzenlenmesini ve her seviyedeki çalışanının uyması gereken kontrol faaliyetlerini iç kontrol yapısı ile sağlarlar [11].

Yasaya göre bankalar, icra görevi olmayan yönetim kurulu üyeleri arasından seçecekleri en az iki üyeden oluşan bir denetim kurulu oluşturmak ve bu şekilde denetim ve gözetim faaliyetlerini yerine getirmek zorundadır. Denetim komitesi, bankanın iç kontrol yapısının etkin şekilde çalışmasından ve malî raporların doğru ve zamanında düzenlenmesini sağlamaktan sorumludur.

Bankacılık Denetim ve Düzenleme Kurulu (BDDK) "Bankaların iç denetim ve risk yönetimi sistemleri hakkında yönetmelik"i 08.02.2001 tarihli ve 24312 sayılı Resmi Gazete'de yayınlamıştır. İç kontrol, iç denetim ve risk yönetimi sistemlerine ilişkin detaylı yönlendirmelerin yer aldığı bu yönetmelik daha sonra kaldırılarak yerine 01.11.2006 tarihli ve 26333 sayılı Resmi gazete'de yayınlanan "Bankaların iç sistemleri hakkında yönetmelik" yayınlanmıştır. Bu düzenleme ile etkin bir iç kontrol yapısının özellikleri, bağımsız denetçinin bu kapsamdaki sorumlulukları ve denetim sürecinde dikkate alınması gereken unsurlar sıralanmıştır.

14 Şubat 2011 tarihinde yürürlüğe giren 6102 sayılı Türk Ticaret Kanunu'nda işletmelerin sahip olması gereken iç kontrol yapısı ile ilgili doğrudan bilgi bulunmamakta ve bu konuda yönetim kurulu üyelerine de bir sorumluluk yüklenmemektedir. Söz konusu kanunda kurumsal risk yönetiminin gerekliliği vurgulandığından, iç kontrol yapısının gerekli olduğunun da dolaylı olarak kabul edildiği düşünülebilir. Zira etkin bir iç kontrol yapısı, risk yönetiminin temelini oluşturmaktadır. Yasada yönetim kurulunun görev ve yetkileri tanımlanırken tedbirli olmak ve dürüstlük kavramlarının yanı sıra yönetime talimatlar vermesi, yönetim teşkilatının belirlenmesi, muhasebe, malî denetim düzeninin kurulması, imza yetkileri, pay ve yönetim kurulu defterlerinin tutulması gibi görevlerden bahsedilmiştir. Ayrıca yasanın 378. Maddesinde "Riskin erken saptanması ve yönetimi" başlığı altında, sadece payları borsada işlem gören şirketlerde yönetim kurulu üyeleri arasından "Riskin yönetilmesi amacıyla bir komitenin" kurulması istenirken, diğer şirketlerde bu konu zorunlu tutulmamış, denetçinin gerekli görüp yönetim kuruluna yazılı olarak bildirmesi durumunda kurulacağı belirtilmiştir.

III. Risklerin Değerlendirilmesi

III.1. Riskin ve Risk Yönetiminin Tanımı

Risklerin değerlendirilmesi COSO iç kontrol modelinin ikinci unsuru olarak yer almaktadır. İlk unsur olan iç kontrol ortamı, içsel ve dışsal unsurları dikkate alarak iç kontrolün nasıl bir çerçeveye oturduğunu açıklarken, risklerin değerlendirilmesi ise doğrudan eyleme dönük bir unsur olarak dikkat çekmektedir.

Her işletme gerek içsel, gerek dışsal risklere maruz kalmaktadır. Risk, burada işletmenin hedeflerini gerçekleştirmesini engelleme ihtimali olan unsurlar olarak değerlendirilmektedir. Amaç ve hedeflerin gerçekleşmesini olumsuz etkileyebileceği değerlendirilen olaylar risk, amaç ve hedefler üzerinde olumlu etkide bulunabileceği değerlendirilen olaylar ise fırsat olarak tanımlanır [10].

Risklerin değerlendirilmesi, işletmenin hedeflerini gerçekleştirmesini engelleme ihtimali olan risklerin belirlenmesi ve değerlendirilmesi faaliyetleridir [2].

Riskler işletmenin başarılı olma kabiliyetini, içinde bulunduğu kesimdeki rekabetçilik seviyesini, malî olarak ve marka değeri açısından güçlü kalabilmesini ve ürettiği ürün ve hizmetlerin kalite düzeyini belirlemesi açısından önemlidir. Risklerin tamamen ortadan kaldırılması mümkün değildir. Her iş, belirli riskleri içerir. İşletme yöneticileri hangi risklerin ne ölçüde kabul edilmesi ve hangi seviyenin üzerindeki risklerin kabul edilmemesi gerektiğini belirlemelidir.

Kurumsal risk yönetimi, kurumun amaç ve hedeflerine ulaşabilmesi açısından makul güvence sağlamaya yönelik yönetsel bir araçtır. Bu nedenle risk yönetimi süreciyle stratejik planlama süreci eş zamanlı olarak yürütülmelidir. Kurumlar öncelikle stratejik planda gösterilen amaçları gerçekleştirmek için hedefler ile riskler arasında bir denge kurup, belirlenmiş olan risk iştahları çerçevesinde hedeflerini belirlerler. Risk yönetiminin aşamaları, risklerin tanımlanması, belirlenmiş olan risklerin niteliksel ve niceliksel (quantitative and qualitative) olarak değerlendirilmesi, risklerin önem ve öncelik sırasının belirlenmesi ve risklere karşılık verme planının yapılması ve risklerin izlenmesinden oluşur [10].

Risk yönetimi, kontrol altına alınması gereken riskleri kontrol altına almak ve yararlanılması gereken fırsatlardan yararlanabilmek için taktiksel ve uzun vadeli kararların alınmasıdır. Risk yönetimi, risklerin ölçülüp rakamlarla ifade edilmesini de içerir, işletme çalışanlarını, faaliyet süreçlerini ve kurumsal yapıyı yönetmeyi de. Risk yönetimi sadece risklere karşı gereken önlemlerin alınması değil, aynı zamanda kurum içinde riskle ilgili bilinç oluşturup esnek, düzenli ve etkin işleyişe sahip süreçler oluşturup bu yapının sürekli güncellenmesini de içerir [14].

Risk yönetimi, kurumun amaçlarını gerçekleştirmek üzere makul bir güvence sağlamak amacıyla potansiyel olay ve durumları belirlemek, değerlendirmek, yönetmek ve kontrol etme sürecidir [15].

24.12.2013 tarihli ve 28861 sayılı resmi gazetede yayınlanan "Bağımsız denetimin planlanması ve yürütülmesinde önemlilik hakkında tebliğ" (BDS 320) risklerin değerlendirilmesi tanımlanmıştır. BDS 320'ye göre bağımsız denetçi denetim planını yaparken, önemli olarak nitelendirilebilecek yanlışlıkların büyüklüğü hakkında muhakemede bulunur. Bu muhakemeler, işletmenin risk değerlendirme prosedürlerinin nitelik, zamanlama ve kapsamının belirlenmesi, önemli yanlışlık risklerinin belirlenip değerlendirilmesi ve denetim tekniklerinin niteliğinin, zamanlama ve kapsamının belirlenmesine dayanak oluşturur [16].

Yukarıda bahsedilen aynı tarihli ve sayılı resmi gazetede yayınlanan "Bağımsız denetçinin değerlendirilmiş risklere karşı yapacağı işler hakkında tebliğ" (BDS 330) malî tabloların denetiminde bağımsız denetçi tarafından belirlenip değerlendirilen önemli yanlışlık risklerine karşı denetçinin yapacağı işler ve sorumluluklarını düzenlemiştir. Bağımsız denetçinin yapacağı işler, önemli yanlışlık risklerine karşılık uygulanacak denetim prosedürleri, sunum ve açıklamanın yeterliliği, denetim kanıtlarının yeterlilik ve uygunluğu ve belgelendirme konularını içerir [17].

III.2. Risklerin Değerlendirilmesinin Aşamaları

Risk yönetimi, işletmelerin uzun vadeli kapsamlı planlarının ayrılmaz bir parçasıdır. İşletmenin her faaliyetiyle ilgili risklerin belirlenmesinin yanı sıra faaliyetler bir araya geldiğinde oluşan bileşik riskleri de değerlendirir.

Risklerin değerlendirilmesi, kurumun hedeflerine ulaşmasını etkileyebilecek faktörlerin analiz edilmesi ve riskin etki ve olasılık açısından öneminin değerlendirilmesidir. Risklerin değerlendirilmesi, riskler tespit edildikten sonra risklerin ölçülmesi, önceliklendirilmesi ve kaydedilmesi aşamalarını kapsar [10].

Risklerin değerlenmesi, her seviyedeki riskin nasıl yönetileceğinin belirlenmesi için gereken zemini hazırlar. Risk değerlemenin temelinde ise, işletmenin farklı hiyerarşik seviyelerdeki hedefleriyle risklerin ilişkilendirilmesi (risk related objectives) gelmektedir. Bununla birlikte, işletmenin maruz kalabileceği risklerin farklı nitelikleri nedeniyle, işletme yönetimi faaliyetlerle ilgili, raporlamayla ilgili ve önceden belirlenmiş kurallara ve yönetmeliklere uyum ile ilgili risk hedeflerini açık ve net bir şekilde belirlemelidir. Bu sayede söz konusu faaliyetler ile ilişkili risklerin belirlenmesi ve analiz edilmesi mümkün olur. Yönetim, ayrıca belirlemiş olduğu hedeflerin işletmeye uygunluğunu da dikkatlice değerlendirmelidir. Ek olarak yönetimin, gerek dış çevredeki gelişmelerin, gerekse işletmenin iş akışlarında meydana gelebilecek değişikliklerin işletmenin iç kontrol yapısına olası olumsuz etkilerini de dikkate alan bir risk değerlendirme sürecine ihtiyacı bulunmaktadır [2].

COSO'nun belirlemiş olduğu ana risk değerlendirme ilkeleri şunlardır:

- Hedeflerin belirlenmesi: İşletmenin hedefleri kesin bir şekilde belirlenmeli, bu hedeflere ilişkin riskler net bir şekilde tanımlanmalı ve olası etkileri değerlendirilmelidir.

- Risklerin belirlenmesi ve incelenmesi (değerlendirilmesi): Risklerin nasıl yönetileceğinin belirlenebilmesi için, işletmenin tüm hedeflerinin başarıyla gerçekleştirilebilmesini etkileyebilecek risklerin belirlenmesi ve incelenmesi gereklidir. Bu aşamaya işletme faaliyet dökümünün yapılması, risk belirleme çalışmasının yapılması, riskler arası ilişkilerin belirlenmesi, risk belirleme faaliyetinin yenilenmesi ve risk analizinin yapılması dahildir.

- Hile riskinin değerlendirilmesi: İşletme hedeflerini gerçekleştirirken maruz kalınabilecek hile riskleri de dikkate alınmalıdır.

- Risklere karşılık (cevap) verilmesi: Risklerin belirlenip değerlendirilmesi ve önceliklendirilmesinden sonra bu risklere nasıl cevap verileceğinin belirlenmesi gereklidir.

III.2.1. Hedeflerin Belirlenmesi

Risklerin değerlendirilmesinde ilk ve en önemli adım, işletmenin riske maruz kalacak hedeflerinin net bir şekilde belirlenmesidir. Bu sayede belirlenen bu hedeflerle ilgili risklerin neler olduğu ve olası etkileri de tahmin edilebilecektir. Buradaki önemli kavram, "risk hedefi" dir. Perakende sektöründe faaliyet gösteren bir işletme için risk hedeflerine örnekler şu şekilde verilebilir:

- Yeni bir yurt dışı pazara rakiplerden önce girebilmek,

- Stokların elde tutulma süresini 90 günden 60 güne indirebilmek,

- Raporlama faaliyetini Excel ortamından güvenilir bir yönetim raporlama yazılım ortamına taşıyabilmek,

- Yabancı para cinsinden yükümlülüklerden kaynaklı kur riskini azaltabilmek için uygun malî araçlar kullanmak.

İşletmenin yönetimi risk hedeflerini net olarak belirlediğinde; işletmenin ana faaliyet hedeflerine ulaşabilmek için mevcut kaynaklarından ne kadarını hangi önceliğe göre kullanması gerektiğini de belirleyebilir. Hedefler kesinlikle malî ve istatistikî somut verilere dayalı olarak belirlenmelidir. Aksi halde, işletmenin kaynaklarının verimsiz kullanılması riski ortaya çıkar.

Risk hedeflerinin belirlenmesi ile ilgili önemli konulardan biri de, işletme faaliyetlerinin tamamını kapsayacak şekilde ele alınmasıdır. Bu şekilde incelendiğinde, işletmenin hedeflerine ulaşmasını engelleme riski olan konular öncelikli olarak dikkate alınmalı ve nasıl yönetilecekleri belirlenmelidir. Ek olarak, önemli riskler ele alındığında gerek hile riski boyutu, gerekse önemlilik kavramı da göz önünde bulundurulmalıdır. Dolayısıyla belirlenmiş olan risk hile riski ise, önleyici faaliyet de söz konusu hilenin yapılmasını önleyici özellikte olmalıdır [2].

Risklerin değerlendirilebilmesi için işletmenin belirlenmiş risk önemlilik sınırlarının (established risk tolerance) olması gereklidir. İşletme yönetimi ve denetçiler, bir hata veya zarar

ortaya çıktığında bunun işletmenin malî tablolarını önemli ölçüde etkileyip etkilemediğini belirleyecek önemlilik ölçütlerini belirlemelidirler.

Bilgi teknolojileri (BT) risklerinin değerlendirilmesi, stratejik etki, hizmet ve faaliyetler, yasal uyum, BT kaynakları ve örgütsel yapı gibi unsurlar çerçevesinde ele alınmaktadır. Risk değerlendirme aşamasında Uluslararası Standartlar Teşkilatı (Intrenational Organization for Standards - ISO) tarafından yayınlanmış olan ISO 31000:2009, Risk Yönetimi – İlkeler ve Kılavuzlar (Risk Management – Principles and Guidelines) standardından da yararlanılabilir.

BT risk değerlendirme süreci, "Kurum seviyesi BT risk değerlendirmesi" ve "Uygulama seviyesi BT risk değerlendirmesi" olarak iki grupta incelenebilir.

Kurum seviyesi BT risk değerlendirmesinde kullanılacak olan kurumsal risk değerlendirme formunda 5 ana başlıkta toplam 31 kapalı uçlu soru sorulur. Beş ana başlık, "stratejik etki", "hizmet ve faaliyetler", "yasal uyum ve mevzuat", "BT kaynakları" ve "örgüt yapısı" unsurlarından oluşur.

Uygulama seviyesi BT risk değerlendirmesi, işletme bünyesinde bulunan uygulamaların temel olarak faaliyetleri ve iş süreçlerini destekleme seviyeleri ve belirli teknik özellikleri açısından değerlendirilmesi amacıyla hazırlanmış olan 16 kapalı uçlu sorudan oluşmaktadır. Değerlendirme yapısı, kurum seviyesi risk puanı için olan ile benzerlik gösterir [18].

Bağımsız denetimde denetçinin; işletmenin malî raporlamayla ilgili faaliyet risklerini bu risklerle ilgili yapılması gerekenler hakkındaki kararlarını ve bu kararların sonucunu tanımlayabilmesi için, öncelikle işltemenin risk değerlendirme sürecini anlaması gerekir. Risk değerlendirme süreci, riskin nasıl tanımlandığı ve yönetildiğini ifade eder [11].

III.2.2. Risklerin Belirlenmesi ve İncelenmesi (Değerlendirilmesi)

Risklerin belirlenmesi süreci, işletmenin tüm faaliyetlerini kapsayacak şekilde maruz kalabileceği tüm risklerin özel bir çalışma yapılarak listelenmesidir. Bu riskler işletmenin bütününü etkileyebilecek büyük çaplı olabileceği gibi, işletmenin belirli faaliyetleriyle veya projelerle sınırlı, daha kısıtlı kapsama dahil de olabilir. Bu süreç aynı zamanda belirlenen risklerden hangilerinin makul bir süre içinde gerçekleşme ihtimalinin yüksek olduğunun belirlenmesini ve gerçekleştiğinde hangilerinin etkisinin önemli olduğunun tespitini de içerir. Bu riskleri belirlerken amaç tüm risklerin listesini çıkarmaktan çok, işletme faaliyetlerini etkileyebilecek risklerin gerçekleşme olasılığı ve gerçekleşme süresi ile ilgili de makul bir tahminde bulunmaktır.

Risklerin belirlenmesi ile ilgili adımlar şunlardır [2].

A. Faaliyet dökümü: İşletmenin sahip olduğu tüm adreslerdeki bütün faaliyetlerinin dökümünü yapmaktır.

B. Risk belirleme çalışmasının yapılması: Listelenen her faaliyete ilişkili risklerin belirlenmesi.

Bu çalışmanın işletme hiyerarşisi içerisinde olabildiğince alt seviyelere kadar indirilmesi, konuya farklı seviyelerden bakılarak bütünsel bir resmin ortaya çıkarılması önerilmektedir. İşletmenin pazarlama yöneticisi, ürünlerin pazarda konumlanması, tüketici algısının yönetilmesi, fiyatların belirlenmesi, satış kanalları ve tanıtım faaliyetlerini kapsayan riskleri ön plana çıkarırken, bilgi sistemleri yöneticisi ise işletme verilerinin yedeklenmesi, sistem arızalarının süratle giderilmesi, virüs saldırılarına karşı korunma yöntemleri gibi konuları dikkate alabilmelidir. Bu iki yönetici de aynı işletmede çalışmalarına rağmen, mevcut risklere oldukça farklı açılardan bakabilmektedir. Üst yönetim ise, birim yöneticilerinin farkında olmayabileceği birçok farklı seviyedeki risk kümelerini belirleyebilir. Bu nedenle, işletmenin farklı birimleri ve örgütün değişik seviyelerindeki çalışanları, riskleri belirleme çalışmasına katılmalıdır.

Risklerin belirlenmesi çalışmasının verimli ve etkin olarak yapılabilmesi için, farklı yöntem ve teknikler kullanılabilir. Aşağıdaki tablo, bir işletmenin maruz kalabileceği risklerin belirli alt bölümler düzeyinde dökümünü göstermektedir. Bu tablodaki riskler örnek olarak listelenmiş olup, her işletme için farklılık gösterir.

Tablo 1. Örnek Risk Tasnifi Tablosu

Stratejik riskler		
Dışsal unsurlar	**İçsel unsurlar**	
-İktisadî ortam riskleri	-İşletmenin güvenilirliği ve piyasadaki marka algısına yönelik riskler	
-İş koluna özgü riskler	-Uzun vadeli hedefler ile ilgili riskler	
-Rekabet riskleri	-Ana şirketin desteği ile ilgili riskler	
-Yasa ve mevzuat değişimi riskleri	-Marka ve isim haklarıyla ilgili riskler	
-Müşteri tercihlerindeki değişim riskleri		
Faaliyetlerle ilgili riskler (Operational risks)		
İş akışı riskleri (Process risks)	**Uyum riskleri (Compliance risks)**	**Çalışanlarla ilgili riskler (People risks)**
-Tedarik zinciri riskleri	-Çevresel riskler	-İnsan kaynakları riskleri
-Müşteri tatmini riskleri	-Mevzuat riskleri	-Personel dönüş hızı (employee turnover) riski
-İş döngü süresi (cycle time) riskleri	-Politika ve prosedür riskleri	-Etkinlik teşvik sistemleri riski
-İş akışı gerçekleştirme (process execution) riskleri	-Yargı süreci (litigation) riskleri	-Eğitim riski

Malî riskler		
Hazine riskleri (Treasury risks)	**Alacak riskleri (Credit risk)**	**Ticaret riskleri (Trading risks)**
-Faiz oranı riski	-Müşteri başına kredi limiti belirleme riski	-Emtia fiyatları riski
-Döviz kuru riski	-Teminat riski	-Vade (duration) riski
-Sermaye yeterliliği riski	-Az sayıda müşteriye bağımlılık (Concentration) riski	-Ölçüm (measurement) riski
	-Alacak tahsil edememe (default) riski	
	-Uyuşmazlık riski	
Bilgi riskleri		
Malî riskler	**Faaliyet riskleri**	**Teknoloji riskleri**
-Muhasebe standartları riski	-Fiyatlama riski	-Bilgiye ulaşım riski
-Bütçeleme riski	-Etkinlik ölçüm riski	-İş sürekliliği (business continuity) riski
-Malî raporlama (financial reporting) riski	-Çalışan güvenliği riski	-Bulunabilirlik (availability) riski
-Vergisel riskler		-Altyapı (infrastructure) riski
-Yasal malî raporlama (regulatory reporting) riski		

Kaynak: [2].

Yukarıdaki liste, ortaklar kurulu toplantısında sorulan genel bir sorunun cevabı olabilir: "Günlük faliyetler sırasında sizi kaygılandıran neler var?" Dolayısıyla bu listeyi, işletmenin karşılaştığı olası tüm risklerin bir sıralanmasından çok, risklerin belirlenmesi çalışmasına başlangıç noktası olarak kabul etmek gerekir.

C. Riskler arası ilişkilerin belirlenmesi: İşletme yönetimi ana risk sınıflarının yukarıdaki örnekte olduğu gibi belirlenmesinden sonra, belirlenen bu sınıflar arasındaki ilişkiyi netleştirmeye çalışmalıdır.

Ürünler, hizmetler ve bilgi akışı arasındaki bağlantılar, işletme içi süreçler içindeki risk etkileşimleri ve işletmenin çevresiyle ilişkili riskler arasındaki bağlantılar ortaya çıkarılmalıdır. İşletme çevresi kapsamına; işletmenin tüm paydaşları girmektedir. Bunlardan bazıları işletmenin müşterileri, bayileri, satış kanalı üyeleri, tedarikçileri, resmi kurumlar, yatırımcılar, kredi veren kuruluşlar, hissedarlar ve rakiplerdir. Bunların yanı sıra işletme yönetimi yasal mevzuattaki değişikliklerin, çevresel mevzuattaki gelişmelerin ve olası doğal afetlerin işletmeye olası etkilerini ve diğer risklerle etkileşimini dikkate almalıdır.

Risklerin belirlenmesi süreci, işletmenin planlama faaliyetleriyle paralel yürütülmelidir. COSO modeli, risklerin belirlenmesi sürecinin önyargılardan ve geçmiş olumsuz deneyimlerden fazla etkilenmeden bağımsız bir bakış açısıyla yürütülmesi gerektiğini öngörür. Bu sayede işletme için geçmişte önemli olarak değerlendirilmemiş bazı risklerin, geçen zaman içinde çeşitli değişim ve gelişmelerle birlikte önemli riskler sınıfına girebileceğini, yani işletmenin hedeflerini gerçekleştirmesini engelleyebilecek boyuta gelmiş olabileceğini dikkate almak gereklidir.

Riskler belirlenirken, işletmenin tüm birimlerinin işin içinde olması gerektiği belirtilmişti. Bunun yanı sıra COSO modeli, işletme dışında olup işletmeyle yakından ilişki içinde olan önemli müşteriler, büyük çaplı alım yapılan tedarikçiler ve satış kanalındaki etkin üyeler gibi dışsal paydaşlardan kaynaklanabilecek risklerin de dikkate alınmasının önemine vurgu yapmaktadır.

D. Risk belirleme faaliyetinin yenilenmesi: Risklerin gözden geçirilme sürecinin hem dinamik (sürekli) bir faaliyet olması, hem de bu çalışmanın belirli aralıklarla geniş bir katılımla yenilenmesi gereklidir. Belirli risk sınıflarının nitelikleri itibariyle çok sık değişime uğramaması nedeniyle sürekli gözden geçirilmesi gerekmeyebileceği gibi, bazı risklerin de faaliyetlerle yakından bağlantılı olması ve sıklıkla değişime uğraması nedeniyle sıklıkla gözden geçirilmesi gerekebilir. İçsel ve dışsal risk unsurlarının belirlenmesi sayesinde yönetim bu unsurların hangisinin ne oranda gerçekleşme ihtimali olduğu ve gerçekleştiğinde etkisinin ne olabileceği konusunda değerlendirme yapabilir ve bu unsurlarla işletme faaliyetlerinin bağlantısını belirleyebilir.

Dışsal risk unsurlarına örnekler:

- Doğal afetler, savaş, terör gibi etkenler nedeniyle hammaddeye erişimin kısıtlanması, emtia fiyatlarındaki dalgalanmalar, bilgi sistemleri altyapısının çökmesi nedeniyle "iş sürekliliği planı"na ihtiyaç duyulması,

- Haksız rekabeti engelleyici mevzuattaki değişimler nedeniyle ürün geliştirme, üretim, fiyatlandırma, müşteri hizmetleri ve satış sonrası hizmet süreçlerindeki değişim ihtiyacı,

- Teknolojideki değişimler nedeniyle işletme için çok önemli verilere ulaşımın zorlaşması, bilgi sistemleri altyapı maliyetlerinin artması.

İçsel risk unsurlarına örnekler:

- Yönetim kademesindeki yetki ve sorumluluk seviyelerindeki değişiklikler nedeniyle iç kontrol yapısında meydana gelen değişimler,

- İşletme faaliyetlerinin niteliği itibariyle ve çalışanların işletme varlıklarına erişimi kapsamında işletme varlıklarının çalınması riski,

- Bilgi sistemleri altyapısında yaşanabilecek aksaklıklar nedeniyle işletmenin faaliyetlerinin kesintiye uğrama riski.

E. Risk incelemesi (analizi) yapılması: İşletme genelinde ve faaliyetler bağlamında riskler belirlendikten sonra risk incelemesi (değerlendirmesi) yapılması gereklidir. Risklerin birçoğunu rakamsallaştırmak karmaşık olduğundan, bu aşama oldukça farklı yöntemlerle gerçekleştirilebilir. Bu kapsamdaki risklerin "gerçekleşme olasılığı" ve gerçekleştiğinde yapacağı "etki" belirlenir. COSO, risklerin değerlendirilmesi kapsamında belirli bir yöntem önermemektedir. İşletme yönetimi en uygun yöntemi belirlemekten sorumludur.

Gerçekleşme olasılığı bir yüzde oranı olabileceği gibi, yüksek ihtimal, orta ihtimal ve düşük ihtimal gibi de nitelendirilebilir. Etki ise, risk gerçekleştiğinde işletmenin faaliyet hedeflerinde yapacağı değişimdir. Bir diğer risk nitelendirme unsuru de "riskin değişim hızı" (velocity)'dır. Riskin değişim hızı, işletme içi veya dışındaki unsurlardaki değişim nedeniyle riskin uğrayabileceği değişimin frekansını gösterir. Örneğin modaya dayalı tüketim ürünlerinde müşteri tercihlerindeki değişim çok hızlıyken muhasebe ilkelerindeki değişimler göreceli olarak daha yavaş gerçekleşmektedir.

Risklerin gerçekleşme olasılığı ve gerçekleştiğinde ortaya çıkaracağı etki belirli ölçülerle ölçülüp sıralandıktan sonra aşağıda görüldüğü gibi bir matrise yerleştirilebilir. Matriste mavi olan kısım, işletmenin göz ardı edebileceği riskleri tanımlarken, kırmızı alan ise tam tersine, işletmenin derhal dikkate alması gereken en önemli ve öncelikli riskleri ifade etmektedir. Kırmızı alandaki risklerle ilgili önlemler alındıktan sonra ise sıra sarı alandaki risklere gelmelidir.

	ŞİDDET				
İHTİMAL	1 (Çok Hafif)	2 (Hafif)	3 (Orta Derece)	4 (Ciddi)	5 (Çok Ciddi)
1(Çok Küçük)	Anlamsız 1	Düşük 2	Düşük 3	Düşük 4	Düşük 5
2 (Küçük)	Düşük 2	Düşük 4	Düşük 6	Orta 8	Orta 10
3 (Orta Derece)	Düşük 3	Düşük 6	Orta 9	Orta 12	Yüksek 15
4 (Yüksek)	Düşük 4	Orta 8	Orta 12	Yüksek 16	Yüksek 20
5 (Çok Yüksek)	Düşük 5	Orta 10	Yüksek 15	Yüksek 20	Tolere Edilemez 25

Şekil 2. Risk Değerlendirme Matrisi

Kaynak: [19]

"İçsel risk" (inherent risk) ve "kalıntı risk" (residual risk) kavramları da risk değerleme sürecinde önemli kavramlardandır. Malî denetimde içsel risk, işletmede hiç iç kontrol yapısı olmadığı durumda malî tablolarda önemlilik derecesi yüksek hata olma olasılığıdır. İçsel riskler işletme faaliyetinin ayrılmaz parçasıdır ve faaliyetlerin her seviyesinde bulunmaktadırlar. Kalıntı risk ise, yönetimin risklere karşı belirlediği kontroller uygulamaya alındıktan sonra geriye kalan risktir. Kontroller ne kadar etkin olursa olsun, her zaman kalıntı risk olacağı, tam olarak sıfırlanamayacağı varsayılır [2].

Amerika Birleşik Devletleri'nde halka açık işletmelerin yıllık faaliyet raporlarının başında yönetimin işletmenin maruz kaldığı mevcut önemli risklerini listelemeleri ve bu risklerle ilgili görüşlerini açıklayıp hisse senetlerine yatırım yapan veya yapmayı düşünen yatırımcıları bilgilendirmeleri beklenmektedir. Aşağıdaki örnek, GAP hazır giyim şirketinin 2013 yılı faaliyet raporunda detaylı açıkladığı risklerden bir kısmının konu başlıkları şu şekildedir [20].

-Stratejik hedeflerimizin ve faaliyet modelimizin hayata geçirilmesinde başarısız olabiliriz,

-İktisadî bunalımlardan, doğal afet, salgın hastalık ve siyasal krizlerden etkilenebiliriz,

-Kilit personeli işe alma ve elde tutma konusunda başarılı olamazsak, faaliyetlerimiz olumsuz yönde etkilenebilir,

-Dünyanın çeşitli ülkelerinde genişlememizi sürdürürken döviz risklerinin olduğu ve hakkında fazla bilgi sahibi olmadığımız coğrafyalarda iş yapmayla ilgili riskleri almamızı gerektirmektedir,

-Franchise faaliyetlerimiz, kontrolümüz dahilinde olmayan ve marka değerimizi düşürebilecek riskler içermektedir,

-Gayrimenkul pazarındaki rekabetçi ortam, kira maliyetlerimizi artırabilir; ödemek zorunda kalabileceğimiz azami kira tutarlarını ve sigorta primlerini tahmin edip yönetiyoruz,

-Modayı ve değişen tüketici tercihlerini etkin bir şekilde takip edememek faaliyet sonuçlarımızı olumuz etkiler,

-İthal ürünlerle ilgili olarak tedarikçilerimizin iş ahlakı ilkelerine (code of conduct) uyumda başarısız olmaları nedeniyle faaliyetlerimiz ve marka değerimiz olumsuz etkilenebilir,

-Tedarik zinciri ve ürün planlama sistemimizin verimsizliği nedeniyle optimal stok seviyelerini tutturamayabiliriz,

-Bilgi sistemlerimizdeki güncellemeler veya değişikliklerin iyi yönetilememesi, hizmet aldığımız şirketlerdeki aksaklıklar veya öngörülemeyen olası aksaklıklar faaliyetlerimizi kesintiye uğratabilir,

-Siber saldırı risklerinden korunmak için sürekli artan maliyetlere katlanmak zorunda kalabiliriz,

-Muhasebe standartlarındaki ve yasal mevzuattaki değişimler faaliyetlerimizi ve malî durumumuzu etkileyebilir,

-Gelecek vadelerde yeterli olabilecek nakde ve kısa vadeli ihtiyaçlar için kullanılabilecek kredi limitlerine sahip olmamız gerekli.

III.2.3. Hile Riskinin Değerlendirilmesi

COSO'nun ilk yayınlandığı 1990larda hilenin araştırılması ve hileyi önlemeye yönelik tedbirlerle ilgili bölümler bulunmamaktaydı. İç ve bağımsız denetçiler, hileyi araştırmayla ilgili görev ve sorumluluklarının olmadığını, bu işin kamu kurumlarınca yerine getirilmesi gerektiğini düşünüyorlardı. 2000'li yıllarda ise hileli malî raporlamanın yaygınlaşması ve temelinde hileli malî raporlamanın olduğu iflasların artmasıyla birlikte hileye bakış açısı değişmeye başladı.

COSO'nun yeni sürümünde de hilenin araştırılması ve ortaya çıkarılması ile ilgili standart bulunmamaktadır. Bununla birlikte, COSO'yu destekleyici ve yönlendirici kaynaklar, işletmenin hedeflerini gerçekleştirmesini engelleyebilecek ölçekte hile riskinin olup olmadığına dair yönetimin sorumluluğunu ortaya koymaktadır. Dolayısıyla yönetimin risk değerlendirme sürecine işletmenin varlıklarının korunması ve hileli malî raporlama da dahildir. Ayrıca yönetim, gerek işletme çalışanlarının, gerekse müşteri ve satıcılar gibi işletmeyle yakın ilişki içinde bulunan dışsal paydaşların içinde olabileceği olası rüşvet vakalarının varlığını da araştırmaktan sorumludur.

Hileli malî raporlama, malî raporların kullanıcılarını yanıltmak üzere ve kasıtlı olarak malî raporların değiştirilmesini içerir. Risk değerleme sürecinde hileli malî raporlama olasılığını aşağıdaki şekilde çeşitli açılardan değerlendirmek gereklidir:

a)Malî raporlamada kullanılan tahmin ve muhasebe ilkelerinin uygunluğu,

b)İşletmenin içinde bulunduğu kesime ve coğrafi konuma özgü hile türlerinin varlığı,

c)Hileli davranışları özendirecek türde teşvik paketlerinin bulunması ve bilgi sistemlerinde yetkilendirme ve verilere ulaşım anlamındaki kontrol eksiklikleri,

d)Yönetimin iç kontrol yapısına gösterdiği önem ve iç kontrol yapısını gözden geçirme sıklığı, gözden geçirilmesi gereken önemli maddelerdendir.

Özet olarak ifade etmek gerekirse yönetim, belirli riskleri tespit eden, inceleyip değerlendiren ve gerekli karşılık verme yöntemlerini belirleyen bir iç kontrol yapısını oluşturmaktan sorumludur. Bu kapsamda yönetim hilenin varlığını ve işletmenin hedeflerine ulaşmasını engelleme seviyesini belirleyecek bir iç kontrol yapısı kurmaktan sorumludur. Yönetimin hileyle mücadele sorumluluğu, COSO iç kontrol yapısı içinde önemli bir yere sahiptir.

III.2.4. Risklere Karşılık (Cevap) Verilmesi

Risk yönetimi anlayışı işletmenin riskleri nasıl değerlendirdiğini, risklere nasıl karşılık verdiğini, nasıl izlediğini, dolayısıyla risk algısını şeffaf ve net bir hale getirip yatırım ve faaliyet kararlarında kullanılabilir hale getirmesini içerir. Risklere karşılık verme yöntemleri, risk yönetimi anlayışının en önemli aşamalarından biridir.

İşletmenin hedeflerine ulaşmasını önemli ölçüde engelleme olasılığı olan risklerin değerlendirilmesi tamamlandıktan sonra, bu risklerin nasıl yönetileceğine de karar verilmesi gerekmektedir. Risklerin olası etkisinin belirlenen karşılık verme yöntemleriyle azaltılarak yönetimin ve işletme hissedarlarının kabul edebileceği seviyeye indirilmesi esastır. Bu arada risklere karşılık verme faaliyetlerinin maliyeti de dikkate alınarak gerçekçi kararlar verilmesi gereklidir. Dolayısıyla kalıntı riskin tamamen sıfıra indirilmesi gerekmemektedir.

COSO'nun yenilenmiş iç kontrol yapısı içerisinde dört adet riske karşılık (cevap) verme yöntemi bulunmaktadır:

A.Kaçınmak (avoidance): Bir coğrafi alandaki faaliyetin sonlandırılması, bir iş kolundan çekilme, bir üretim hattının kapatılması bu stratejiye örneklerdir. Uygulanması oldukça maliyetli olabilir. Eğer işletmenin risk iştahı çok düşük seviyelerde değilse, sadece olası bir riskten dolayı belirli bir faaliyetin durdurulması sıklıkla karşılaşılan bir durum değildir. İşletme yönetiminin geçmiş hatalardan ders çıkararak, geçmişte yaşanmış olumsuz durumlara benzer vakalar yaşandığında bu stratejiyi uygulama olasılığı artmaktadır. Çoğunlukla olası risk gerçekleşip bu riskle ilişkili olarak zarar da ortaya çıktıktan ve işletmenin etkinliklerini olumsuz yönde etkiledikten sonra bu karar verilmektedir.

B.Azaltmak (reduction): İşletme faaliyetleri dahilinde yönetimin inisiyatifiyle ve başka bir kuruluşu devreye sokmaya gerek olmadan yapılabilecek faaliyetleri kapsar. Birçok işletme kararı belirli risklerin düşürülmesine yardım etmektedir. Örneğin üretim hattının çeşitlendirilmesi, bir tek ürüne bağımlı olma sorununu ortadan kaldırabilir, bilgi sistemleri sunucularının farklı coğrafi bölgelere yerleştirilmesi, doğal âfet durumunda oluşabilecek zararları azaltır.

C.Paylaşmak (sharing): İşletme dışından kuruluşların devreye sokulmasıyla uygulanan bir yöntemdir. Neredeyse bütün işletmeler sigorta poliçeleri satın alarak mevcut risklerini azaltmakta veya risklerini paylaşmaktadırlar (hedge or share). Birçok farklı türde riski paylaşma yöntemi daha bulunmaktadır. Malî işlemlerle ilgili olarak işletmeler vadeli işlem sözleşmesi ve opsiyon sözleşmesi benzeri riskten korunma (hedging) araçlarını kullanmaktadırlar. Bir diğer paylaşma enstrümanı da işletmeler arasında yapılan ortak iş girişimleridir.

D.Kabul etmek (acceptance): Bu yöntem hiç bir önlem almamak olarak özetlenebilir. İşletmeler risklerin olası sonuçlarını tahmin ederek risk tahammül seviyeleri dahilindeyse kabul edebilirler.

İşletme yönetimi risklere karşılık verme yöntemleri olarak bu dört seçenekten birini tercih etmelidir. Bu yöntemlerden birini seçerken de işletmenin risk iştahını dikkate alarak maliyet

ve getiri hesabı yapmalıdır. Risk iştahı, kurumun kabul etmeye istekli olduğu risk seviyesidir [15]. Birçok durumda da hangi riske nasıl karşılık verileceği konusunda iş dünyasında belirli bir fikir birliği bulunmaktadır. Örneğin hangi risklere karşılık sigorta poliçesi satın alınacağı bellidir. Ayrıca bilgi sistemleri altyapısının ve verilerin güvenliğinin sağlanması için yapılması gereken faaliyetler de bilgi sistemleri yöneticilerince bilinmektedir.

Riske karşılık verme uygulamaları temelde şu aşamalardan oluşmaktadır:

a) Riske karşılık verecek kişi veya birimin belirlenmesi,

b) Riske karşılık verme kararları arasındaki ilişkinin netleştirilmesi,

c) Diğer unsurlar ile riske karşılık verme kararları arasındaki ilişkinin belirlenmesi,

d) Uygulama zaman planının belirlenmesi,

e) Riske karşılık verme yönteminin verimliliğinin ölçülmesi ile ilgili planın yapılması,

f) Riskleri izlemeyi tetikleyen unsurların belirlenmesi,

g) Bazı durumlarda, risklere karşılık verme ile ilgili ara dönem ölçümlemeleri de belirlenmelidir.

Risklere karşılık vermek, risklerin her birine karşılık hangi yöntemin kullanılacağını belirleyen örgütsel bir yaklaşımdır. İşletmeler bazı durumlarda üst yönetimin kabul edebileceği tahammül sınırlarını aşan riskleri almış olabilirler. Bu durumda, risk seviyesinin çeşitli riskten kaçınma yöntemleriyle azaltılması için harekete geçmek gereklidir. Yönetimin riski karşılamaya yönelik kontrol faaliyetleri de dahil, aldığı tedbirlerden sonra kalan riske artık risk (residual risk) denir [15]. Riskten kaçınma yöntemleri, işletmenin sınırlı kaynaklarının kullanımı anlamına geleceğinden, verimsiz işlemlere girişmemek için riskten kaçınmak için katlanılan maliyet ve riskin azalma derecesi kıyaslanmalıdır. Riske karşılık verme uygulaması, işletmenin hedeflerine ve uzun vadeli hedeflerine uygun risk temelli kararlar verilmesine yardımcı olarak üst yönetimi güçlendirmektedir.

III.3. COSO Risk Değerlendirme ve Güncellenmiş İç Kontrol Yapısı

COSO'nun iç kontrol yapısına ilişkin ilkeleri ilk günden günümüze kadar fazla değişikliğe uğramamıştır. Bununla birlikte destekleyici iç kontrol yönergeleri (supporting internal control guidance) önemli ölçüde değişmiştir.

İşletmenin risk değerlendirme süreci tüm ana faaliyetlerini, uyum faaliyetlerini ve raporlama ihtiyaçlarını içermelidir.

Önemli kavramlardan biri de işletmenin risk kabul seviyesi, veya toleransıdır. Bu kavramı netleştirmek için şu iki soruyu sormak gereklidir:

a) İşletmenin hedeflerini gerçekleştirebilmesi için yatırım yapabileceği kaynağı ne kadardır?

b) İşletme ne kadarlık kayba tahammül edebilir?

Bu iki sorunun cevabını en iyi verecek kurum, işletmenin yönetim kuruludur. Yönetim kurulu işletmenin risk iştah seviyesi, risk felsefesi ve risk tutumu konularında net bir mutabakata varmakla yükümlüdür.

Risk değerlendirme faaliyetleri sonucu belirlenen hedefler ile uyumlu olarak işletmenin malî durumu ve faaliyetlerle ilgili etkinliğine dair hedefleri belirlenmelidir. Yönetim de bu etkinlik hedeflerine ulaşabilmek için kaynakları en uygun şekilde tahsis etmekle yükümlüdür.

IV. SONUÇ

İşletmeler için kalıcı başarıya ulaşabilmenin ön koşullarından biri, riskleri iyi yönetebilmektir. Risk olmadan kazanç sağlamak mümün değilken, alınan ölçüsüz riskler de işletmenin sonunu getirebilir. Gelişip büyümek ve faaliyetlerini çeşitlendirerek yeni pazarlara girmak isteyen işletmelerin etkin bir iç kontrol yapısına sahip olması gereklidir. Etkin bir iç kontrol yapsının en önemli unsurlarından biri de risklerin tespiti ve değerlendirilmesidir.

İç kontrol yapısının önemi dünya genelinde tüm iş kollarında, ve kamu kurumlarında gittikçe artmaktadır. İç kontrol kavramının önemini artıran unsurlardan biri faaliyetleri çeşitlenip coğrafi olarak genişleyen işletmelerin ihtiyaç duyduğu kurumsal yönetim yapısı, diğeri de gelişen iletişim ve teknolojiyle paralel olarak çeşitlenen ve etkileri artan risklerdir. Kurumsal yönetimin temel unsurlarından biri kurumsal risk yönetimidir. Kurumsal risk yönetimi de temelinde iç kontrol yapısını barındırmaktadır. Dolayısıyla iç kontrol yapısı işletmelerin hedeflerine ulaşabilmek için sahip olmaları gereken en temel unsurlardan biridir.

Özellikle ABD, Kanada, Birleşik Krallık gibi Anglosakson kültüre sahip ülkelerde geleneksel olarak iç kontrol kavramının diğer ülkelerdekinden daha geniş bir anlamı ifade etmesi, bu ülkelere aynı zamanda bir çok alanda rekabet üstünlüğü de getirmektedir. Bunun farkına varan Kıta Avrupası ülkeleri, Uzak Doğu Asya ülkeleri ve gelişmekte olan ülkeler de yasal mevzuatlarına iç kontrol kavramını gittikçe artan oranda yansıtmaktadırlar.

Ülkemizde şimdilik sadece halka açık şirketlerin ve bankaların etkin bir iç kontrol yapısına sahip olması yasal bir gerekliliktir. Ülkemizin dünyanın en büyük ekonomileri arasına girebilmesi ve işletmelerimizin ürettiği ürün ve hizmetlerin dış pazarlarda rekabet üstünlüğünü sağlayabilmesi için bilinçli, etkin ve verimli yönetilmeleri, işletme varlıklarının kötüye kullanımının engellenmesi, faaliyet sonuçlarının hızlı ve doğru şekilde raporlanabilmesi ve mevzuata uyum konusundaki yetkinliklerinin üst düzeyde olması gereklidir. Bu da etkin bir iç kontrol yapısıyla mümkündür. Etkin bir iç kontrol yapısının ülkemizde tüm işletmelerde vaz geçilmez bir unsur haline gelmesi için de gerek yasal düzenlemelerle zorunlu hale getirilmesi, gerekse çeşitli unsurlarla teşvik edilmesi yararlı olacaktır.

Yararlanılan Kaynaklar

[1] Türedi, Hasan. (2015). Genel Muhasebe. Trabzon: Celepler Matbaacılık Yayın ve Dağıtım.

[2] Moeller, R. Robert. (2014). Executive's Guide to COSO Internal Controls-Understanding and Implementing the New Framework. New Jersey: John Wiley & Sons Inc.

[3] Özbek, Çetin. (2012). İç Denetim, Kurumsal Yönetim, Risk Yönetimi, İç Kontrol. İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.

[4] Güredin, Ersin. (2014). Denetim ve Güvence Hizmetleri, SMM ve YMM'lere Yönelik İlkeler ve Teknikler. İstanbul: Türkmen Kitabevi

[5] Arens, A. Alvin, Elder, J. Randal, Beasley, S. Mark. (2014). Auditing and Assurance Services, an Integrated Approach. Essex: Pearson Education Limited.

[6] Uluslararası Denetim Standartları. UDS 200. UDS 200: Bağımsız Denetçinin Genel Amaçları ve Bağımsız Denetimin Uluslararası Denetim Standartlarına Uygun Olarak Gerçekleştirilmesi. KGK (Kamu Gözetimi Kurumu)

[7] Türedi, Hasan. (2000). Denetim. Trabzon: Celepler Matbaacılık Yayın ve Dağıtım.

[8] Türedi, Hasan. Karakaya, Gencay. İldem, Mehmet. (2015). Kurumsal Yönetim ve İç Denetim İlişkisi. Sayıştay Dergisi, Sayı: 96, ss. 96

[9] Türedi, Hasan. Gürbüz, Filiz. Alıcı, Ümmügülsüm. COSO Modeli: İç Kontrol Yapısı. Marmara Üniversitesi Öneri Dergisi, Cilt 11, Sayı 42, ss. 141-155.

[10] T.C. Maliye Bakanlığı Bütçe ve Kontrol Genel Müdürlüğü. Kamu İç Kontrol Rehberi. Ankara: 2014.

[11] Aksoy, Tamer. (2010). Derecelendirme ve Kurumsal Yönetim Süreci ile KOBİ'ler, Bankalar ve Kurumsal İşletmeler Işığında Basel ve İç Kontrol. Ankara: TÜRMOB Yayınları, Grup Matbaacılık A.Ş.

[12] Sermaye Piyasası Kurumu (SPK). (2015). II-17.1 Sayılı Kurumsal Yönetim Tebliği. 03.01.2014 tarihli, 2887103 Sayılı Resmi Gazete.

[13] Bankacılık Denetleme ve Düzenleme Kurulu (BDDK). (2015). 5411 Sayılı Bankacılık Kanunu. 01.11.2005 tarihli, 25983 Sayılı Resmi Gazete,

[14] Coleman, S, Thomas. (2011). A Practical Guide to Risk Management. London: The Research Foundation of Certified Financial Advisor (CFE) Institute.

[15] Türkiye İç Denetim Enstitüsü. www.tide.org.tr

[16] Uluslararası Denetim Standartları. UDS 320. UDS 320: Bağımsız denetimin planlanması ve yürütülmesinde önemlilik. KGK (Kamu Gözetimi Kurumu)

[17] Uluslararası Denetim Standartları. UDS 330. UDS 330: Bağımsız denetçinin değerlendirilmiş risklere karşı yapacağı işler. KGK (Kamu Gözetimi Kurumu)

[18] T.C. Maliye Bakanlığı İç Denetim Koordinasyon Kurulu. Kamu Bilgi Teknolojileri Denetim Rehberi. Ankara: 2013

[19] İş Güvenliği Çevre Kalite Eğitim Danışmanlık Tic. Ltd. Şti. Internet Sitesi. www.isguv.com.tr

[20] GAP Inc. Year 2014 Annual Report. Internet Sitesi. www.gapinc.com

Hasan TÜREDİ - hturedi@ticaret.edu.tr

Received his master of business administration degree from İstanbul University and PhD in accounting, auditing and finance from Karadeniz Teknik University. He is currently a faculty member in the Department of Business Administration at İstanbul Ticaret University. He teaches accounting, internal auditing, internal controls and fraud audit.

Ahmet Oğuz KOBAN - okoban61@gmail.com

Received his MBA from Koç University, currently a PhD student in İstanbul Ticaret University in the field of accounting and auditing. He holds a SMMM certificate (certified public accountant). His research interests include internal control, risk management, auditing and corporate governance.