Marmara Üniversitesi Öneri Dergisi • Cilt 11, Sayı 42, Temmuz 2014, ISSN 1300-0845, ss. 141-155
DOI: 10.14783/ÖNERI.2014427000

COSO MODELİ: İÇ KONTROL YAPISI

Hasan TÜREDİ*
Filiz GÜRBÜZ**
Ümmügülsüm ALICI***

Özet

İktisadi ve teknolojik gelişmeler; zaman içinde çok sayıda faaliyetin çok sayıda kişi ve uzun süreçlerle yürütüldüğü, hiyerarşik örgütsel düzenlerin sürekli geliştiği, karmaşık işletme yapılarının ortaya çıkmasına neden olmuştur. Bunun sonucunda işletmelerin faaliyetleri basit kontrol yöntemleriyle izlenemeyecek hale gelmiştir. Amerika'da beş bağımsız meslek kuruluşundan oluşan COSO (The Committe of Sponsoring Organizations), iç kontrolün işletmelerde standartlaşan bir yapı hale gelmesinde öncülük etmiştir. COSO iç kontrol modeli; iç kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim ile izleme faaliyetlerinden oluşan; işletme faaliyetlerinin etkinliği ve verimliliği, mali raporların güvenilirliği ve yürürlükteki kanun ve düzenlemelerle uyum amaçları etrafında şekillenmiş çok boyutlu bir yapıdır. İç kontrol yapısının başlıca hedefleri; faaliyetlerin etkinlik ve verimliliği, karlılık hedefine ulaşmak ve varlıkların korunması, kamuya açıklanan mali tablolar, geçici ve özet mali raporları da dâhil olmak üzere hazırlanan tüm mali tabloların güvenilirliğinin sağlanması ve tabi olunan kanun ve düzenlemelerle uyumun sağlanmasıdır. Bu çalışmada; COSO'nun iç kontrol yapısına ilişkin geliştirdiği model ve bu modelin beş bileşeni olan kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim ile izleme faaliyetleri aracılığı ile bu bileşenlerin hem işletme hedefleri hem de işletme yapısı içindeki etkileşimi açıklanmaya çalışılmıştır.

Anahtar Kelimeler: COSO, İç Kontrol, Risk Yönetimi, Kontrol Faaliyetleri.
Jel Sınıflaması: M 10, M 40, M 42

COSO MODEL: INTERNAL CONTROL STRUCTURE

Abstract

Developments in economy and technology have caused enterprises to have sophisticated structures affected by developing hierarchical structuring along with the significant number of activities performed

* Prof. Dr, İstanbul Ticaret Üniversitesi, Ticari Bilimler Fakültesi, Muhasebe ve Denetim Bölümü.
** Doktora Öğrencisi, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Bölümü.
*** Doktora Öğrencisi, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Bölümü.

via significant number of process and individuals. COSO (The Committee of Sponsoring Organizations) has established a common internal control model against which companies and organizations may assess their control systems. Internal control model is a multidimensional structure with the five components which are control environment, risk assessment, control activities, information and communication and monitoring. These interrelated components have been developed with the objectives regarding effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations. This study aims to explain the internal control model developed by COSO as well as with the five components which are control environment, risk assessment, control activities, information and communication and monitoring along with their interrelationship.

Keywords: COSO, Internal Control, Risk Management, Control Activities.

1. Giriş

İktisadi ve teknolojik gelişmeler sonucunda, işletmeler büyük ve karmaşık yapılar haline gelmiş, çalışan kademeleri çeşitlenmiş ve işletmelerin faaliyetleri basit kontrol yöntemleriyle izlenemeyecek duruma gelmiştir. Geçmişte tek bir kişinin kontrolü, bir işletmedeki faaliyetlerin, planlandığı şekilde yürütüldüğünden emin olmak için yeterliyken, günümüzde işletme faaliyetlerin işletme hedefleriyle uyum içinde olmasını sağlamak için, bir işletmede yönetim kurulu dâhil tüm çalışan kademelerinin dâhil olduğu kapsamlı, örgütlü ve ayrıntılı bir kontrol yapısına olan ihtiyaç kaçınılmaz hale gelmiştir.

Amerika'da beş bağımsız meslek kuruluşundan oluşan COSO (The Committe of Sponsoring Organizations), iç kontrolün işletmelerde standartlaşan bir yapı hale gelmesinde öncülük etmiştir. Bugün tüm dünyada COSO İç Kontrol Modeli, işletme hedeflerine ulaşmak için yürütülen faaliyetlerin düzenli bir şekilde kontrol edilmesi için gerekli yapıların tasarlanmasını, risklerin değerlendirilmesini ve işletme faaliyetlerinin sürekli bir şekilde kontrol altında tutulmasını sağlayan bir model olarak ortaya çıkmıştır.

COSO iç kontrol modeli; iç kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim ile izleme faaliyetlerinden oluşan; işletme faaliyetlerinin etkinliği ve verimliliği, mali raporların güvenilirliği ve yürürlükteki kanun ve düzenlemelerle uyum amaçları etrafında şekillenmiş çok boyutlu bir yapıdır.

2. COSO (The Committe of Sponsoring Organizations) İç Kontrol Modeli

2.1. Genel Açıklamalar

Treadway Komisyonu olarak da adlandırılan COSO (The Committe of Sponsoring Organizations), Amerika'da beş bağımsız meslek örgütü tarafından kurulmuştur. Amerikan Muhasebeciler Birliği(AAA), Amerika Sertifikalı Kamu Muhasebecileri Birliği (AICPA) ,Uluslararası Finans Yöneticileri(FEI), İç Denetçiler Enstitüsü(IIA) ve Yönetim Muhasebecileri Enstitüsü (IMA) 'nün oluşturduğu COSO Komitesi; 1985 yılında kurulmuştur ve amacı hileli mali raporlamayla mücadele amacıyla kurulmuştur [1].

Coso, 1992 yılında;

- Faaliyetlerin etkinlik ve verimliliği,
- Mali raporların güvenilirliği,
- Yürürlükteki kanun ve mevzuata uygunluk olmak üzere üç ana başlık altında,

İç kontrol, kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ve izleme olmak üzere beş bileşenden oluşan, İç Kontrol- Bütünleşik Çerçeve'yi (Internal Control-Integrated Framework) yayımlamıştır (COSO, 1992). Yayımlanan bu çerçeve geniş bir kabul görmüş ve günümüzde dünya üzerinde yaygın olarak uygulanmaktadır. Ayrıca; COSO, 2004 yılında iç kontrol yapısını geliştirerek mali raporların (tabloların) güvenilirliğinin sağlanması amacıyla işletmenin hedeflerine başarıyla ulaşabilmesinde ortaya çıkabilecek kurumsal risk boyutunun tanımlandığı Kurumsal Risk Yönetimi Bütünleşik Çerçevesini (KRY-Enterprise Risk Management -ERM) yayımlamıştır [2].

1992 yılında yayımlanan İç Kontrol Bütünleşik Çerçeve'nin üç ana başlık ve beş bileşenine sadık kalınarak PricewaterhouseCoopers denetim ve danışmanlık şirketi tarafından hazırlanan, kavramların açıklanması ve kullanımın kolaylaştırması bakımından iç kontrol yapısında olması gereken niteliklerin ve 17 adet ilkenin eklenmesiyle önemli iyileştirmeler yapılarak, 2011 yılında güncelleştirilerek yeniden yayımlanmıştır [3].

1992 yılından günümüze kadar şirketlerdeki kurumsallaşma yapılarının değişmesi, iş ve çalışma ortamlarındaki değişiklikler, pazarlama ve faaliyetlerle ilgili olarak gelişen teknoloji ve küresel değişiklikler, yolsuzlukların tespit edilerek önlenebilmesi ile ilgili beklentiler, değişen yasalar ve mevzuata uyum sağlanması ve işletmelerin iç kontrol yapısını güncel tutmak amacıyla COSO iç kontrole ilişkin çalışmalarını düzenli olarak güncellemeyi sürdürmektedir.

2.2. İç Kontrol

İç kontrol; işletmeler, kanun koyucu ve düzenleyiciler ile diğer kişiler açısından farklı anlamlar taşımaktadır. Bir şirkette iletişim eksikliği ve beklentilerin farklı olması sorunlara neden olmaktadır. İç kontrol, bir işletmenin yönetim kurulu, üst yönetim ve diğer çalışanları tarafından etkilenen ve işletmenin temel hedeflerinin yerine getirildiğine dair makul bir güvencenin elde edilmesini sağlayan geniş bir yapıdır [1].

Makul güvence; Yüksek düzeyde bir güvencedir. Denetim riskini(Denetçinin mali tabloların sunumu hatalı iken uygun olmayan bir denetim görüşü verme riski)azaltmak için denetçinin yeterli ve uygun denetim kanıtını elde ederek denetim riskini kabul edilebilir seviyeye indirmesidir[4].

Bir İşletmedeki Hedefler aşağıdaki şekilde sıralanabilir:

- Faaliyetlerin etkinliği ve verimliliği,
- Mali raporların (tabloların) güvenilirliği,
- Yürürlükteki kanun ve diğer düzenlemelere uyum

Bir işletmenin temel hedefi; **faaliyetlerin etkinlik ve verimliliği**, karlılık hedefine ulaşmak **ve varlıkların korunmasıdır.** İkinci hedefi kamuya yayınlanan mali tabloların ve raporların, geçici

ve özet mali raporları da dâhil olmak üzere hazırlanan **tüm mali raporların güvenilirliğinin sağlanmasıdır.** Üçüncüsü ise **işletmenin tabi olduğu kanun ve yönetmeliklere uyumun sağlanmasıdır.**

İç kontrol yapısının genel çerçevesini aşağıdaki gibi sınıflandırmak mümkündür [3].

- İç kontrol, görev ve faaliyetlerin sürekli olarak devam ettiği dinamik ve tekrarlanan bir yapıdır.
- Bir işletmenin her kademesinde çalışan insanlar tarafından etkilenir.
- İşletmenin üst yönetimi ve yönetim kuruluna kesin bir güvence vermez, makul güvence sağlar.
- Bir veya daha fazla hedefe ulaşılmasına bağlı olarak işletmelerin yapılarına göre farklı sınıflara ayrılabilir
- İşletme yapılarına göre uyarlanabilir.

3. İç Kontrollerin Bütünleşik Çerçevesi

İç kontrol yapısı birbiriyle ilişkili beş bileşenden oluşmaktadır:

- Kontrol ortamı,
- Risk değerlendirme,
- Kontrol faaliyetleri,
- Bilgi ve iletişim,
- İzleme.

Bu bileşenlerle ilgili özet bilgiler aşağıda verilmiştir.

3.1. Kontrol Ortamı

Kontrol ortamı, şirket çalışanlarının kontrol bilincini etkileyen bir çalışma ortamı oluşturmasının yanı sıra bir disiplin ve temel oluşturur. Meslek ahlakı, şirket çalışanlarının yeterliliği, yönetim felsefesi ve çalışma tarzı, yönetimin yetki ve sorumluluklarının dağılımı, şirket çalışanlarının geliştirilmesi(eğitimi) ve örgütlenmesi, yönetim kurulu tarafından sağlanan yönlendirme ve faaliyetlere gösterilen özen gibi unsurlar kontrol ortamını oluşturur [5].

İç kontrol yapısının temel bileşenlerinden biri olan kontrol ortamı; bir şirketin geçmişi, benimsediği meslek ahlak değerleri, dürüstlüğü, faaliyet gösterdiği piyasa, rekabet koşulları ve yasal düzenlemeler gibi çeşitli iç ve dış faktörlerden etkilenir [3].

Kontrol ortamının unsurları olan ilkeler, bir işletmede iç kontrol yapısının yürütülebilmesi ve işletme hedeflerine ulaşılabilmesi için temel sağlamaktadır [3].

Kontrol ortamı; aşağıdaki ilkelerden oluşmaktadır.

- Dürüstlük ve meslek ahlakı,
- Yönetim kurulunun iç kontrol faaliyetlerini gözetim sorumluluğu,
- Görev ve yetki dağılımlarının belirlenmesi,

- Yetkinlik Taahhüdünün Tesisi, Çalışanların teşviki ve geliştirilmesinin (eğitim, eğitimin sürdürülmesi, uzmanlaşma) tesisi,
- Yetki ve sorumluluklar.

3.1.1. Kontrol Ortamının İlkeleri

3.1.1.1. Dürüstlük Ve Meslek Ahlakı

Yönetim kurulu ve üst yönetim, talimatları, davranışları ve faaliyetleri ile işletmenin her kademesinde iç kontrol yapısının işleyişinde dürüstlük ve meslek ahlakı ile ilgili değerlerin önemli olduğuna ve sürdürülmesi gerektiğine ilişkin bir tutum sergilemelidirler. Yönetim kurulu ve üst yönetim, dürüstlük ve meslek ahlakı ile ilgili davranış standartları (kuralları) belirlemeli ve bu kuralların işletmenin her kademesi, dışarıdan hizmet sağlayanlar ve iş ortakları tarafından anlaşılmasını sağlamalıdır. Şirket tarafından, bireylerin ve çalışanların beklenen davranış kurallarına bağlılıkları değerlendirilerek, bir sapma var ise zamanında ve uygun bir şekilde belirlenerek giderilmelidir [3].

3.1.1.2. Yönetim Kurulunun İç Kontrol Faaliyetlerini Gözetim Sorumluluğu

Yönetim kurulu; tarafsız, yönetimden bağımsız, nitelikli ve yeterli sayıda üyeye sahip olmalıdır**.** Yönetim kurulu kendi üyelerinin bilgi, beceri ve uzmanlıklarını tanımlayarak belirli aralıklarla değerlendirmeler yapar. Bundan amaç, gerektiğinde üst yönetimi sorgulayabilmek ve gerekli tedbirleri alabilmektir [3].

Gözetim sorumluluğu yönetim kuruluna aittir. Amaçlanan hedeflerde başarıya ulaşılabilmesi için yönetim kurulu gözetim sorumluluğunu üstlenir ya da üst düzey yöneticilere bu amaçla yetki verir. Yönetim kurulu iç kontrol yapısının etkinlik ve verimliği ile işleyişini takip eder, yönetir ve kılavuzluk yapar [3].

3.1.1.3. Görev Ve Yetki Dağılımlarının Oluşturulması

Üst yönetim ve yönetim kurulu, belirlenen amaçlara ulaşabilmek için işletmenin tüm birimleri, yasal düzenlemeler ve dış kaynak hizmet sağlayıcıları (bağımsız denetim, mali danışmanlık, eğitim vb) da dâhil olmak üzere tüm yapıları göz önünde bulundurmalıdır [3].

Yönetim, işletme faaliyetlerinin sürdürülebilmesi için işletmenin her kademesinde bilgi akışı, sorumluluklar ve yetkilerin yerine getirilebilmesini sağlamak amacıyla raporlamaların ne şekilde yapılacağına ilişkin iletişim hatlarını (raporlama akışı) belirler ve değerlendirir [3].

Yönetim kurulu, yönetim ve işletmenin her kademesinde yetki ve sorumluların tespiti, yetkilendirme, yetkileri sınırlandırma ve sorumluluk atamalarını, görevlerin ayrılığı ilkesine uygun olarak belirler [3].

3.1.1.4. Yetkinlik Taahhüdünün (Çalışanların Teşviki Ve Geliştirilmesinin) Tesisi

İşletme hedeflerinde başarıya ulaşabilmek için ihtiyaç duyulduğunda; dışarıdan hizmet sağlayanlar ile nitelikli ve yetenekli personel için, rehberlik ve eğitim hizmeti sağlar. Üst yönetim ve yönetim kurulu tarafından politika ve uygulamalar tesis edilerek işletmenin geneli ve dışarıdan

hizmet sağlayanların yetkinlikleri değerlendirilir, gerek duyulduğunda eksikliklerin giderilmesi için önlemler alınır. [3].

Üst yönetim ve yönetim kurulu iç kontrol sorumlularının atamalarında, gelecekte yapılacak görevlendirmeler ve ortaya çıkabilecek beklenmedik durumlar için durum planları geliştirirler [3].

3.1.1.5. Yetki Ve Sorumluluklar

İşletme hedeflerine ulaşılmasında, tüm çalışanların iç kontrol yapısının işleyişinden sorumlu tutularak hesap verilebilirlikleri sağlanır. Yönetim ve yönetim kurulu, iç kontrol yapısının etkin ve verimli çalışabilmesi için bireylerin sorumlulukları ve iletişimin tesis edilmesini, gerekli durumlarda düzeltici önlemeler alınmasını sağlar. Hedeflere ulaşılmasına yönelik baskılar var ise değerlendirmeler yapılarak gerekli önlemler alınır. Yönetim ve yönetim kurulu, iç kontrol yapısının sorumluluklarının yerine getirilmesi, kısa ve uzun vadede başarıya ulaşılabilmesini teşvik etmek amacıyla, işletmenin her kademesinde, beklenen davranış kurallarına bağlılıkları, yetkinlik beklenti seviyelerini, etkinlik ve verimliliğin ölçümünü ve değerlendirmesini yaparak uygun bir şekilde ödüllendirme ya da disiplin tedbirleri (cezalandırıcı) alır **[1]**.

Kontrol Ortamına Yönelik İlkeler

Temel İlkeler	**Ayrıntılar**
Dürüstlük Ve Meslek Ahlakı	Yönetimin tutumu. Davranış kurallarının belirlenmesi, Davranış kurallarına bağlılıkların değerlendirilmesi, Sapmalara zamanında müdahale
Yönetim Kurulunun İç Kontrol Faaliyetlerini Gözetim Sorumluluğu	Gözetim sorumluluklarının belirlenmesi, İlgili uzmanlık uygulaması, Faaliyetlerde bağımsızlık. Kontrol ortamının gözlemlenmesi,
Görev Ve Yetki Dağılımlarının Oluşturulması	İşletmenin tüm yapısını göz önünde bulundurma. Raporlama hatlarının tesisi (raporlama akışı). Yetki ve sorumluluk atamaları ve sınırlandırmalar.
Yetkinlik Taahhüdünün (Çalışanların Teşviki Ve Geliştirilmesinin)Tesisi	Politika ve uygulamaların oluşturulması, Yetkinliklerin değerlendirilerek eksikliklerin giderilmesi, Çalışanların Geliştirilmesi (sürekli eğitim). Planlama ve hazırlık.
Yetki Ve Sorumluluklar	Yetkili ve sorumluların hesap verebilirliği (hesap verebilir olmaları). Verimlilik ve etkinliğin ölçümü, ödüllendirme, teşvik. Devam eden ilginin değerlendirilmesi, teşvik ve ödüllendirme. Baskıların göz önünde bulundurulması, Verimlilik ve etkinliklerin değerlendirilmesi bireyleri ödüllendirme ya da disiplin uygulamaları.

Kaynak: [1].*Internal Control- Integrated Framework.COSO. 2013*

3.2. Risk Değerlendirmesi

Her işletme iç veya dış kaynaklardan gelebilecek neden olabileceği birçok riskle karşı karşıyadır. İşletmeler açısından risk; gerçekleşmesi halinde, işletmeyi hedeflerine ulaşması bakımından olumsuz etkiyebilecek bir olay veya olaylar olarak tanımlanabilir [**6**]. İşletmeler hedeflerine ulaşabilmek için karşı karşıya oldukları riskleri başarılı bir şekilde yönetmek zorundadır. Risk yönetimi; bir işletmenin yönetim kurulu, yöneticileri ve çalışanlarının aktif bir şekilde rol aldığı bir süreçtir. Bu süreçte risk olarak değerlendirilebilecek olaylar tanımlanır, belirlenen risklere karşı işletmenin risk kabul düzeyi ortaya konulur ve riskin kabul edilebilirlik düzeyi çerçevesinde riske karşılık(önlem alınır) verilir. Riske verilen karşılık; riskin kabul düzeyine göre; riskin kabul edilmesi, riskin azaltılması, riskin paylaşılması veya riskten sakınma şeklinde olabilir [2]. COSO'nun iç kontrol bileşenleri içinde risk değerlendirme faaliyetlerine yönelik ilkeleri ise aşağıdaki tabloda verilmiştir.

Risk Değerlendirmesine Yönelik İlkeleri

Temel İlkeler	Ayrıntılar
Hedeflerin Belirlenmesi	İşletme hedeflerine ilişkin risklerin tanımlanmasını ve değerlendirilmesini sağlamak için hedeflerin net bir biçimde belirtilmesi.
Risklerin Belirlenmesi ve Analiz Edilmesi	İşletme genelinde hedeflere ulaşabilmek için hedeflere ilişkin risklerin belirlenerek en makul risk yönetim sürecinin oluşturulması.
Hile Riskinin Değerlendirilmesi	Hedeflere ilişkin risk yönetim sürecinde hile riskinin ele alınması.
Risklerde Meydana Gelebilecek Değişimlerin İzlenmesi	İşletmenin iç kontrol yapısının mevcut risklerdeki değişimlerle uyumlu olmasını sağlamak amacıyla risklerde meydana gelebilecek değişimlerin izlenmesi.

Kaynak: [1].*Internal Control- Integrated Framework.COSO. 2013*

3.2.1. Hedeflerin Belirlenmesi

Bir işletmede başarılı bir risk yönetim sürecinin oluşturulmasının ilk adımı gerçekçi ve ulaşılabilir hedeflerin ortaya konmasıdır. İşletmelerin başlıca hedefi kar elde etmek ve büyümektir. Bu hedeflere ulaşmak için faaliyetler sürdürülürken farklı alt hedefler belirlenmektedir. Örneğin bir işletme, piyasaya yeni bir ürün sunmayı amaçlıyorsa bunun için gerekli üretim hattının oluşturulması, bu üretim hattında görev alacak kalifiye personelin istihdam edilmesi gibi alt hedefler de belirlenecektir. İşletmeler açısından risk değerlendirmesi; işletme bakımından stratejik öneme sahip amaçlara ulaşmak için faaliyet gösterilirken gerçekleşmesi halinde, işletmeyi etkileyebilecek risklerin önceden belirlenmesi ve gerekli önlemlerin alınması sürecidir. Yapılan

çalışmalar; risklerin belirlenmesi, değerlendirilmesi ve bu risklere gerekli karşılıkların verilmesi hususunda risk yönetim süreçleri tesis eden işletmelerin belirledikleri hedeflere ulaşmada, diğerlerine oranla daha başarılı olduklarını göstermiştir [7].

3.2.3. Olay Tanımlaması

İşletmeler faaliyetlerini sürdürürken birçok farklı olay, fırsat veya risk unsuru olabilmektedir. Örneğin yurt dışından hammadde temin eden bir işletme için döviz kurunda ani bir artış risk unsuruyken, yurtdışına satış yapan bir işletme için bu bir fırsat unsuru olabilir. Dolayısıyla işletmelerde belirlenen hedeflere ulaşılmasına etki edebilecek olaylar belirlenmeli ve bu olaylar risk veya fırsat olarak bir değerlendirmeye tabi tutulmalıdır.

Bir işletmede riski ele alırken dikkat edilecek en önemli hususlardan biri, riskin türüdür. İşletmelerin karşı karşıya oldukları ve yönetmeleri gereken riskler; doğal risk ve kalıntı risk olmak üzere iki grupta incelenir. **Doğal risk** işletmenin hiç bir önlem almadığı takdirde ortaya çıkan risktir. **Kalıntı risk** ise doğal riske karşı işletmenin önlem aldıktan sonra dahi karşı karşıya kaldığı risk türüdür. Risk değerlendirmesi iki boyutlu bir süreçtir. Bir işletmede risk ele alınırken hem oluşma hem de etkisi bakımından ele alınmalıdır [8].

Etkin bir risk yönetimi için risk teşkil edebilecek olayları tanımlarken, işletmeler birçok farklı tekniğe başvurabilirler. Olaylar listesi, atölye çalışmaları, anketler, süreç akım analizleri bu tekniklere örnek verilebilir [2].

3.2.4. Kabul Edilebilir Risk Düzeyi

İşletmeler belirlenmiş hedefleri açısından birçok riskle karşı karşıyadır. Risk değerlendirmesi yapılırken, risklerin önemlilik derecesine göre(cevap, önlem) karşılık verilir. Örneğin; büyük oranda insan gücüne dayalı üretim yapan 9000 personele sahip bir işletmede 5 personelin işten ayrılması özellikle önlem alınması geren düzeyde bir risk değilken, 15 personele sahip bir başka işletme için acilen karşılık verilmesi gereken bir risk olabilir. Bir olay, benzer faaliyetlerde bulunan işletmelerin tamamı için bir risk teşkil etse de riskin etki düzeyi her bir işletme bakımından farklı olacaktır. Başarılı bir risk yönetimi için risklere karşılık vermeden önce riskin ne ölçüde makul olduğunun belirlenmesi gerekmektedir [2].

3.2.5. Riske Karşılık Verilmesi

Riskin tanımlaması, oluşumu ve etkisi bakımından ele alınması neticesinde riske ne şekilde karşılık verileceği belirlenebilir. Kabul edilebilir risk düzeyine göre bir işletme riski kabul edebilir, riski azaltma ya da paylaşma yoluna gidebilir veya riskten kaçınmayı seçebilir [9]. Birçok risk için işletmeler bu seçenekleri birlikte kullanabilirler. Bunlar aşağıda özetlenmiştir.

3.2.5.1. Riskin Kabulü

Belirlenen bir risk, meydana gelme veya etkisi bakımından işletmenin kabul edilebilir risk sınırları içinde yer alıyorsa, işletme bu riski kabul etme yoluna gidebilir. Örneğin bir inşaat işletmesi için bir binanın inşa aşamasında deprem olma ihtimali bir risktir veya bir üretim işletmesi için sipariş iptali, bir risk olarak görülebilir. İşletme alınan toplam sipariş miktarının

%5'ine kadar bir iptali makul bulmaktadır. Bu işletmenin alınan toplam siparişleri 1 ton ise bu işletme için 50 kg'ın altında bir sipariş iptali kabul edilebilir. Risk değerlendirme sürecinde işletmeler genellikle kabul edilebilir risk düzeyi dışında kalan riske karşı önlem almakta ve alınan önlemden sonra, kalıntı risk kabul edilebilir risk düzeyi içinde ise bunu kabul etmektedir [10].

3.2.5.2. Riskin Azaltılması

Kabul edilebilir risk düzeyi dışında kalan riskin oluşma ve/veya etkisine karşı, riskin azaltılmasına yönelik önlemler en yaygın risk karşılığıdır. Burada riskin gerçekleşme ihtimaline karşı bir önlem almak mümkün olmasa bile etkilerini azaltmaya yönelik önlemler alınabilir. Örneğin; bir inşaat işletmesi için depremin gerçekleşme ihtimalini azaltmak mümkün değildir fakat depreme dayanıklı binalar inşa etmek ve bu binaları depreme karşı sigortalatmak deprem riskinin etkilerini azaltmak için alınabilecek önlemlerden bazılarıdır [2].

3.2.5.3. Riskin Paylaşılması

Bazı durumlarda işletmeler kendileri için risk teşkil edebilecek bir olayın gerçekleşmesi durumunda, katlanacakları maliyetleri paylaşmayı seçebilirler. Örneğin; bir nakliye işletmesi, karayolu nakliyesi sırasında trafik kazası olması halinde taşınan malların zarar görmesine karşı müşterisinden malların olası bir kazaya karşı sigortalatmasını talep edebilir [2].

3.2.5.4. Riskten Sakınma

Risk değerlendirmesi sonucunda belirlenen bir riskin gerçekleşme ihtimaline karşı işletmeler riskten kaçınma yoluna gidebilirler. Örneğin; piyasa için çok yeni olan bir ürün; işletme açısından yüksek maliyetli bir üretim hattı kurulmasını gerektiriyorsa ve işletme üretime karar verme aşamasında yaptığı risk değerlendirmesi sonucunda, yeni ürünün talep görmemesi halinde, mali olarak dar boğaza girecekse bu ürünün üretiminden vazgeçebilir [2].

3.3. Kontrol Faaliyetleri

İç kontrol yapısı dâhilinde işletmede sürdürülen faaliyetler sistematik bir yapının döngüleridir. Bu yapı çerçevesinde kontrol ortamı ya da risk değerlendirme sürecinde yürütülen faaliyetlerde devamlılık esastır. Bu nedenle; işletmede iç kontrol yapısı çerçevesinde tanımlanan her bir süreç ya da uygulamanın planlandığı şekilde yürütülmesinden emin olmak için bazı politika ve süreçler geliştirilmelidir. Bir işletmede tanımlanan kontrol faaliyetleri, işletmenin hedeflerine göre sınıflandırılabilir. İşletmenin ana hedefi veya ana hedefe ilişkin ortaya konulan alt hedeflere göre; faaliyetler, mali raporlama ve mevcut kanun ve düzenlemelerle uyumlu olabilir [2].

Yetkilendirme, onay, doğrulama, faaliyetlerin etkinlik ve verimliliğinin gözden geçirilmesi, varlıkların güvenliğinin(korunması) sağlanması (fiziki kontroller) ve görevlerin ayrılığı gibi birçok kontrol faaliyeti, işletmenin her düzeyde belirlediği risklere karşı yürütülen kontrol faaliyetlerinden bazılarıdır. Bu faaliyetlerin başarılı olabilmesi, bütünleşik bir iç kontrol yapısının işletmenin tüm kademelerinde ve tüm faaliyetlerini kapsayacak şekilde yürütülmesine bağlıdır [**1**]. COSO'nun kontrol faaliyetlerine yönelik uyulması gereken ilkeler ise aşağıdaki tabloda verilmiştir.

Kontrol Faaliyetlerine Yönelik İlkeleri

Temel İlkeler	Ayrıntılar
Kontrol Faaliyetlerinin Seçilmesi ve Uygulamaya Konulması	İşletme hedeflerine yönelik mevcut risklerin kabul edilebilir düzeylerde olmasını sağlamak için en uygun kontrol faaliyetlerinin seçilmesi ve uygulamaya konulması.
Teknoloji Tabanlı Genel Kontrollerin Uygulamaya Konulması	İşletmenin genelinde hedeflere ulaşabilmek için teknoloji destekli genel kontrollerin oluşturulması.
Politika ve Süreçlerin Geliştirilmesi	İşletme hedeflerine ulaşabilmek için kontrol faaliyetlerinin politika ve süreçlerle desteklenmesi.

Kaynak: [1].*Internal Control- Integrated Framework.COSO. 2013*

3.3.1. Risk Değerlendirmesiyle Kontrol Faaliyetleri Arasındaki İlişki

Kontrol faaliyetleri iç kontrol yapısını tüm yönleriyle destekleyen faaliyetler olmasına karşın, özellikle risk değerlendirme süreciyle bütünleşik olarak yürütülür. Risk değerlendirme sürecinde belirlenen risklerin gerçekleşme ihtimali veya etkilerine karşı işletmenin tavrı; riskin kabul edilmesi veya riskin paylaşılması olduğunda genellikle, ayrıca bir kontrol faaliyetine ihtiyaç duyulmamaktadır. Bununla birlikte; riskten sakınılması veya riskin azaltılması söz konusu olduğunda belirlenen riske karşılık olarak kontrol faaliyetleri kullanılabilir [3]. Örneğin bir işletme stok kayıplarını risk olarak değerlendiriyorsa, bunu önlemek için; nakil evraklarının depo müdürü tarafından kontrol edilip onaylanmasını sağlayarak hem süreklilik arz edecek bir kontrol faaliyeti gerçekleştirmiş hem de belirlediği riske karşılık vermiş olur [2].

Kontrol faaliyetleri belirlenirken; işletmenin hedeflerine ulaşmak üzere faaliyet gösterirken karşılaşabileceği risklerin en aza indirilmesi, ortaya konan kontrol faaliyetlerinin işletmenin politikaları içinde yer alması gerekmektedir [3].

3.3.2. İşletmeye Özgü Kontrol Faaliyetleri

Her işletme farklı hedeflere ulaşmak üzere kendine özgü faaliyetler sürdürmektedir. İşletmenin faaliyet alanı, faaliyet yerleri, çalışanları, büyüklüğü, örgüt yapısı gibi birçok farklı etken kontrol faaliyetlerine de yansıyacağından bu faaliyetler işletmeye özgü bir şekilde gelişecektir [3].

Başarılı bir kontrol faaliyetinin sahip olması gereken özelliklerden bazıları şunladır [2]:

- Faaliyetlerle ilgili kritik noktalar üzerinde durulmalı,
- İç kontrol yapısıyla bütünleşik bir şekilde tanımlanmalı ve yürütülmeli,
- Güvenilir ve tutarlı bilgi sağlamalı,
- İç kontroller kolaylıkla uygulamaya konabilmeli,
- Kontrol uygulamasının maliyeti; riskin işletmeye getireceği maliyeti geçmeyecek düzeyde olmalıdır [2].

3.3.3. Kontrol Faaliyetlerinin Bilgi İşleme Süreçlerine Göre Sınıflandırılması

İşletmelerde ana hedeflere ulaşılmasını sağlayan alt hedefler, çeşitli faaliyet süreçleri aracılığıyla sağlanmaktadır. Her bir hedef, kendine özgü riskler barındırır. Bu riskleri yönetmek için en yaygın yol riskleri bilgi işlemeye ilişkin amaçlarına göre sınıflandırmaktır. Bu sınıflandırma tamlık, doğruluk ve geçerlilik şeklinde yapılabilir. Gerçekleşen her bir işlemin kayıt altında olması, doğru bir şekilde kaydedilmiş olması ve her bir kaydın gerçekleşmiş iktisadi bir işlemi yansıtması bilgi işleme süreçlerinin başlıca hedefleridir [3]. Bilgi işleme süreçleri genel olarak mali raporlamayla ilişkilendirilse de her işletmenin farklı faaliyetlerinde bu süreçler kullanılmaktadır. Örneğin; bir şeker üreticisi; ürettiği şekerlerin içeriklerinin(bulunması gerekli malzeme) üretimde kullanıldığından (tamlık) doğru miktarda içerik kullanıldığından (doğruluk) ve kullanılan malzemelerin kalite kontrolden geçtiği bir tedarikçiden sağlandığından (geçerlilik) emin olmak için farklı kontrol faaliyetleri yürütebilir.

3.4. Bilgi İletişim

Gerekli bilginin zamanında sağlanması ve işletme içinde veya dışında yer alan ilgili kişi ya da kurumlara iletilmesi, iç kontrol yapısının vazgeçilmez bir ilkesidir. Bilgi sistemleri işletme içinde oluşturulmuş veri(bilgi) ve/veya işletme dışından sağlanmış verileri kullanır. Etkin ve verimli bir iletişim sistemi ise elde edilen bilgilerin işletmede gerekli makamlara ulaşmasını sağlar. İletişim sistemleri tüm çalışanların; risk yönetimi ile ilgili sorumluluklarını net bir şekilde öğrenmesini sağlayacak şekilde hizmet vermelidir [2].

İç kontrol yapısıyla ilgili olarak; iç kontrol ortamından başlayarak işletmenin risk yönetim felsefesinin, risk kabul düzeyinin, risk değerlendirme sürecinde görev alan tüm çalışanlara iletilmesi, belirlenen risklere verilecek karşılıklara göre kontrol faaliyetlerinin düzenlenmesi gibi tüm alanlarda, iletişim kesintisiz ve doğru bir şekilde sağlanmalıdır.

Etkin bir iç kontrol yapısı için; kaliteli, zamanında, ulaşılabilir, güvenliği sağlanmış(korumalı) ve doğrulanabilir bilginin sağlanması özellikle bilgi sistemlerinin karmaşık otomasyon yapılarına sahip olduğu günümüz işletmeleri için esastır [3]. Bilgi ve iletişim faaliyetlerine yönelik geliştirilen COSO ilkeleri aşağıdaki tabloda sunulmuştur.

Bilgi ve İletişim Faaliyetlerine Yönelik İlkeleri

Temel İlkeler	Ayrıntılar
Bilginin Değerlendirilmesi	İşletmenin iç kontrol yapısını desteklemek amacıyla ilgili ve kaliteli bilgi toplanması ve kullanılması.
İşletme İçi İletişim Süreçleri	İç kontrol yapısını desteklemek amacıyla iç kontrole ilişkin amaçlar ve sorumluluklar da dâhil olmak üzere gerekli bilginin işletme içi birim ve kişilere iletilmesi.
İşletme Dışı İletişim Süreçleri	İç kontrol faaliyetlerine etki edebilecek konularda işletme dışındaki ilgili kişi ve kurumlarla iletişim süreçlerinin oluşturulması ve sürdürülmesi.

Kaynak: [1].*Internal Control- Integrated Framework.COSO. 2013*

3.4.1. İşletme İçi İletişim

İşletme amaçlarının paylaşılması, işletme içinde sağlanacak iletişimin başlangıç noktasıdır. İşletmenin ana hedeflerinin yönetim tarafından ilgili birimlere sunulması ve bu birimlerin belirleyeceği alt hedeflerin ilgili personele iletilmesi ile başlayan bu süreç işletmenin hiyerarşik yapısı içinde doğru bir şekilde sürdürülmeli, her bölüm ve çalışan kendine ait sorumluluklardan zamanında ve doğru bir şekilde bilgi sahibi olmalıdır. Benzer şekilde risk yönetim süreçlerinde de ilgili personel; amaçlar, riskler, riskin kabul düzeyi, riske verilecek karşılıklar ve kontrol faaliyetleri ile ilgili olarak gerekli bilgileri doğru bir şekilde, doğru zamanda ve doğru kişi ve/veya bölümlerle paylaşmalıdır [3].

Yönetim kurulunun, üst yönetime bağlı kalmaksızın çalışanlarla doğrudan iletişim kurabilmesi de iç kontrol bakımından önemlidir. Yönetim kurulu, üst yönetim olmaksızın alt kademe yönetim ve diğer çalışan kademelerine ulaşarak, üst yönetimin işletmenin ana hedefleri doğrultusunda hareket edip etmediğine dair bilgi sağlayabilir. Böylece kontrol çevresinde bahsi geçen yapı, yetki ve sorumluluklara uygun bir biçimde gerekli bilgilerin iç kontrol yapısına uygun bir şekilde sağlanması mümkün olur.

3.4.2. İşletme Dışı İletişim

İşletme içinde sağlanan iletişim kadar, işletmenin çıkar gruplarıyla olan iletişimi de hedeflere ulaşılması bakımından önemlidir. Hissedarlar, kurumsal ortaklar, müşteriler, tedarikçiler gibi farklı çıkar gruplarıyla sağlanacak etkin ve verimli bir iletişim, işletmenin hedeflerine ulaşmasında etkili olur. Örneğin; müşterilerle sağlanan başarılı bir iletişim gelecek siparişlerin yoğunluğunu belirlemede esas oluştururken, tedarikçilerle sağlanan iletişim, zamanında yapılacak teslimatlarla üretim süreçlerinin aksamadan yürütülmesini sağlayabilir.

3.5. İzleme

İç kontrol süreçlerinin başarılı bir şekilde sürdürülmesini sağlamak için bu süreçlerin düzenli olarak izlenmesi ve gerektiğinde güncellemeler yapılması gerekmektedir. İzleme faaliyetleri, bütünleşik bir iç kontrol yapısının tüm bileşenleriyle sürekliliğinin sağlanması, doğru ve zamanında faaliyetlerde bulunulması amacıyla düzenli olarak değerlendirilmelidir. [9].

Bir işletmedeki mevcut iç kontrol yapısı; işletmenin amaçları, iktisadi yaşamdaki değişimler, teknolojik gelişmelere ve değişen üretim süreçlerine bağlı olarak, zaman içinde değişime uğrar. Düzenli olarak yürütülen izleme faaliyetleri ile iç kontrol yapısının değişen koşullara uygun olarak yeniden yapılandırılması sağlanabilir. İşletme birimlerinden sağlanan bilgilerin günlük takibinden, satış tahminlerinin değişen koşullara göre yeniden yapılmasına kadar birçok faaliyet, düzenli izleme faaliyetleri kapsamında sıralanabilir. İzleme faaliyetleri, planlanan ile gerçekleştirilenin, rutin karşılaştırılmasıdır.

İzleme Faaliyetlerine Yönelik İlkeleri

Temel İlkeler	Ayrıntılar
Sürekli İzleme Faaliyetleri ve Gerektiğinde Tesis Edilen İzleme Faaliyetleri	İç kontrol yapısı içinde yer alan bileşenlerin planlandığı şekilde faaliyet gösterildiğinden emin olmak için sürekli ya da koşullara göre tesis edilen izleme faaliyetlerinin yürütülmesi.
Eksikliklerin Değerlendirilmesi ve İlgili Birim ve Kişilere İletilmesi	İç kontrol yapısında eksiklik veya hataların tespit edilmesi ve işletme içinde gerektiğinde yönetim kurulu ve üst yönetim de dâhil olmak üzere ilgili birim ve kişilere iletilmesi.

Kaynak: [1].*Internal Control- Integrated Framework.COSO. 2013*

3.5.1. Süreçlerin Değerlendirmeleri

Faaliyetlerin etkinliğinin sürekli olarak kontrol altında tutulmasını sağlamak amacıyla; izleme faaliyetlerinin yürütülmesinin yanı sıra, iç kontrol bileşenlerinin bireysel(her bir bileşenin) olarak değerlendirmelerini yapabilmek için de izleme faaliyetleri yürütülebilir. İç kontrol bileşenlerinin başarısı, büyük ölçüde değişen koşullara göre güncellenmeleri ve varsa mevcut sorunların zamanında tespit edilmesi ve bunların etkin bir iletişim yoluyla gerekli yönetim kademelerine bildirilmesine bağlıdır [2].

Özellikle risk değerlendirme sürecinde; işletmenin ana hedeflerine ulaşmasını sağlamak amacıyla ortaya konan her alt hedef, bu hedefe ilişkin riskler sürekli olarak değişmektedir. Her çalışma kademesi, her süreç değişen bu koşullara hızla uyumlu hale getirilmelidir. Başarılı bir izleme faaliyeti iç kontrolün tüm bileşenlerinin düzenli olarak takip edilmesini sağlar.

4. Sonuç

Faaliyetlerin etkinlik ve verimliliği, karlılık hedeflerine ulaşmak ve varlıkların korunması, kamuya açıklanan mali tablolar, geçici ve özet mali raporlar da dâhil olmak üzere hazırlanan tüm mali tabloların güvenilirliğinin sağlanması ve tabi olunan kanun ve düzenlemelerle uyumun sağlanması işletmelerin başlıca amaçlarıdır. İşletmenin iç kontrol yapısı bu amaçlara ulaşılırken karşılaşılabilecek risklerin yönetilmesi için temel oluşturmaktadır.

COSO 1992 yılından bu yana teknolojik gelişmeler ve işletmelerin kurumsallaşmaları neticesinde geliştirdiği iç kontrol modelini düzenli olarak güncellemektedir. Böylece ana ilkelere bağlı kalınarak COSO iç kontrol modeli günümüzde iç kontrol yapıları için temel oluşturmaktadır.

İç kontrol, görev ve faaliyetlerin sürekli olarak devam ettiği dinamik ve tekrarlanan bir yapıdır ve işletmenin her kademesinde çalışan insanlar tarafından etkilenir. İç kontrol yapısı; işletmenin üst yönetimi ve yönetim kuruluna kesin bir güvence vermemekle birlikte, makul güvence sağlar. İç kontrol yapısı; ana ilkeleri aynı kalmakla birlikte; işletmelerin büyüklüğü ve faaliyet alanı gibi yapısal özelliklerine göre uyarlanabilir.

COSO iç kontrol modeli; iç kontrol ortamı, risk değerlendirmesi, kontrol faaliyetleri, bilgi ve iletişim ve izleme faaliyetlerinden oluşan; işletme faaliyetlerinin etkinliği ve verimliliği, mali raporların güvenilirliği ve yürürlükteki kanun ve düzenlemelerle uyum amaçları etrafında şekillenmiş çok boyutlu bir yapıdır.

Kontrol ortamı, şirket çalışanlarının kontrol bilincini etkileyen bir çalışma ortamı oluşturmasının yanı sıra bir disiplin ve temel oluşturur. Meslek ahlakı, şirket çalışanlarının yeterliliği, yönetim felsefesi ve çalışma tarzı, yönetimin yetki ve sorumluluklarının dağılımı, şirket çalışanlarının sürekli geliştirilmesi ve örgütlenmesi, yönetim kurulu tarafından sağlanan yönlendirme ve faaliyetlere gösterilen özen gibi unsurlar kontrol ortamını oluşturur.

Risk değerlendirmesi; bir işletmenin yönetim kurulu, yöneticileri ve çalışanlarının aktif bir şekilde rol aldığı bir süreçtir. Bu süreçte risk olarak değerlendirilebilecek olaylar tanımlanır, belirlenen risklere karşı işletmenin risk kabul düzeyi ortaya konulur ve riskin kabul düzeyi çerçevesinde, riske karşılık verilir. Riske verilen karşılık; riskin kabul düzeyine göre; riskin kabul edilmesi, riskin azaltılması, riskin paylaşılması veya riskten sakınma şeklinde olabilir.

Kontrol faaliyetleri; işletmede iç kontrol yapısı çerçevesinde tanımlanan her bir süreç ya da uygulamanın planlandığı şekilde yürütülmesinden emin olmak için geliştirilen politika ve süreçlerdir. Bir işletmede tanımlanan kontrol faaliyetleri işletmenin hedeflerine göre sınıflandırılabilir. İşletmenin ana hedefi veya ana hedefe ilişkin ortaya konulan alt hedeflere göre; faaliyetler, mali raporlama ve mevcut kanun ve düzenlemelerle uyum olabilir. Yetkilendirme, onay verme, doğrulama, faaliyetlerin etkinlik ve verimliliğinin gözden geçirilmesi, varlıkların güvenliğinin (koruma) sağlanması (fiziki kontroller) ve görevlerin ayrılığı gibi birçok faaliyet, işletmenin her düzeyde belirlediği risklere karşı yürütülen faaliyetlerden bazılarıdır. Bu faaliyetlerin başarılı olabilmesi, bütünleşik bir iç kontrol yapısının işletmenin tüm düzeylerinde ve tüm faaliyetlerini kapsayacak şekilde yürütülmesine bağlıdır.

Bilgi ve iletişim süreçleri; işletme içinde oluşturulmuş veri(bilgi) ve/veya işletme dışından sağlanmış verileri kullanır. Etkin ve verimli bir iletişim sistemi ise elde edilen bilgilerin işletmede gerekli mercilere ulaşmasını sağlar. İletişim sistemleri tüm çalışanların risk yönetimi ile ilgili sorumluluklarını net bir şekilde öğrenmesini sağlayacak şekilde hizmet vermelidir.

Düzenli olarak yürütülen izleme faaliyetleri ile iç kontrol yapısının değişen koşullara uygun olarak yeniden yapılandırılması sağlanabilir. İşletme birimlerinde sağlanan bilginin günlük takibinden satış tahminlerinin değişen koşullara göre yeniden yapılmasına kadar birçok faaliyet düzenli izleme faaliyetleri kapsamında sıralanabilir. İzleme faaliyetleri planlanan ile gerçekleştirilenin, rutin olarak karşılaştırılmasıdır. Bunun yanı sıra iç kontrol bileşenlerinin değişen koşullara göre yeniden düzenlenmesi için de her bileşene yönelik olarak yürütülecek izleme faaliyetleri ile güncelleme sağlanabilir.

COSO iç kontrol modeli; birbiri ile etkileşim içindeki bileşenlerin, işletmelerde faaliyetlerin sağlıklı bir şekilde yürütülmesi için gerekli örgütsel altyapıyı oluşturmak, işletmelerin karşı karşıya kaldıkları ya da kalabilecekleri riskleri başarı ile yönetmek ve bu süreçlerin devamlılığını ve güncelliğini sağlamak amacıyla geliştirilmiş bir yapıdır. Gelişen ve değişen iktisadi birimler olarak işletmeler; bu yapı ile risklere karşı kesin bir başarıyı sağlamamakla birlikte, faaliyetlerin etkinlik ve verimliliği, mali tabloların güvenilirliği ve tabi olunan kanun ve düzenlemelerle uyum açısından makul güvence sağlayabilmektedir.

Yararlanılan Kaynaklar

[1] COSO. (2013). *Internal Control — Integrated Framework.* COSO(Commitee of Sponsoring Organizations of the Tradeway Commission).

[2] COSO. (2004). *Enterprise Risk Management- Integrated Framework, Application Techniques* . COSO(Commitee of Sponsoring Organizations of the Tradeway Commission).

[3] COSO. (2011). *Control — Integrated Framework.* COSO (Commitee of Sponsoring Organizations of the Tradeway Commission).

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

[5] COSO. (1992). *Internal Control — Integrated Framework.* COSO(Commitee of Sponsoring Organizations of the Tradeway Commission).

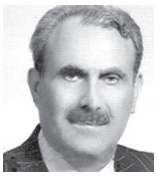
[6] COSO. (2012). *Internal Control — Integrated Framework.* COSO (Commitee of Sponsoring Organizations of the Tradeway Commission).

[7] AICPA. (2008). *A Unified Approach to Risk Management.* AICPA

[8] Beasley, M. S. (2007). *Developing Effective Internal Controls Using the COSO Model.* Raleigh, NC ABD: Enterprise Risk Management Initiative.

[9] Deloitte & Touche LLP. (2012). *Risk Assessment in Practice.* COSO.

[10] AIRMIC & ALARM. (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* AIRMIC (Association of Insurance and Risk Managers).



Hasan TÜREDİ (hturedi@ticaret.edu.tr)

Hasan Türedi is a professor of Faculty of Commercial Sciences, Accounting and Auditing Department in Istanbul Commerce University. Ministry of Finance: Internal Audit Coordination Board members, Member of the Supervisory Board at the Central Bank of Turkey (2010-2014). He has been working on the field of accounting especially in the areas of corporate governance, internal audit, internal control, fraud auditing and international audit standards.

Filiz GÜRBÜZ (gurbuzfiliz@hotmail.com)

Filiz Gürbüz is a PhD student at Istanbul Commerce University. She holds a SMMM certificate (certified public accountant), and currently working on her PhD in the Department of Accounting and Auditing in Istanbul Commerce University. Her research interests include corporate governance, internal audit, internal control.

Ümmügülsüm ALICI (gulsumalici@gmail.com)

Ümmügülsüm Alıcı is a PhD student at Istanbul Commerce University. She holds a MPA degree and currently working on her PhD in the Department of Accounting and Auditing in Istanbul Commerce University. Her research interests include internal control, corporate governance, activity based systems and business intelligence.