Risk Odaklı İç Denetim

Hasan TÜREDİ [*]
Ümmügülsüm ZOR [**]
Filiz GÜRBÜZ [***]

ÖZET

İç denetim bir kurumun ya da işletmenin faaliyetlerini geliştirmek ve onlara değer katmak amacıyla yürütülen bağımsız ve tarafsız(nesnel) bir güvence ve danışmanlık faaliyetidir. İşletmede yürütülen faaliyetler zaman içinde değişen işletme koşullarına bağlı olarak değişime uğramaktadır. İşletmede yürütülen kurumsal yönetim ve iç kontrol gibi işletme içi yapıların ortaya çıkışı ve gelişimi, iç denetim anlayışı ve uygulamalarının da farklı bir boyut kazanmasında etkili olmuştur ve risk odaklı iç denetim anlayışı ve uygulamaları önem kazanmıştır. Risk odaklı iç denetim uygulamaları işletme riskleri üzerinde odaklanarak bu risklerin işletme hedeflerine uygun bir şekilde yönetilebilmesini amaçlamaktadır. Özü itibari ile bakıldığında risk odaklı iç denetimin başlıca görevleri; işletmelerde kurumsal yönetim ve iç kontrol faaliyetlerinin denetlenmesi ve risklerin yönetilmesi konusunda üst yönetime danışmanlık hizmeti sunmaktır. Bu çalışmada ilgili konularda standart belirleyici kurumların yayınları ve genel kabul görmüş uygulama esasları çerçevesinde bir literatür taraması yapılmak suretiyle risk odaklı iç denetimin kavramsal çerçevesi açıklanmaya çalışılmıştır. Ayrıca risk odaklı iç denetimin gelişimi, iç kontrol ve kurumsal yönetim ile ilişkisi ve işleyiş biçimi özet olarak sunulmuştur.

Anahtar Kelimeler: *İşletme Riski, Risk Yönetimi, İç Denetim, İç Kontrol, Kurumsal Yönetim.*

JEL Sınıflandırması: *F20, M40 M42.*

Risk Based Internal Audit

ABSTRACT

Internal auditing is an independent and objective assurance and consulting activity designed to add value and improve an organization's operations. These activities have changed appropriately to changing conditions over time. Emergence and development of internal control and enterprise risk management within enterprises has been effective in gaining a different dimension in internal audit applications. As a difference from traditional internal audit; risk based internal audit focuses on business risks and target managing risk according to the objectives of the enterprise. In this context, the main missions of risk-based internal audit are monitoring internal control and corporate risk management activities and providing advisory services to senior management in respect of risk management. In this study, we tried to explain conceptual framework of risk based internal audit via literature review of publication of related organizations and general accepted applications. Also we aimed to describe relationship among risk based audit; internal control and enterprise risk management as well as how it operates in an enterprise.

Keywords: *Business Risk, Risk Management, Internal Audit, Internal Control, Corporate Governance.*

Jel Classification*: F20, M40 M42.*

[*] Prof. Dr. Hasan Türedi, İstanbul Ticaret Üniversitesi, Ticari Bilimler Fakültesi, hturedi@ticaret.edu.tr
[**] Arş. Gör. Ümmügülsüm Zor, İstanbul Kemerburgaz Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, gulsumalici@gmail.com
*** Filiz Gürbüz, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, gurbuzfiliz@hotmail.com

1. GİRİŞ

Enron, WorldCom, Parmalat vb. şirketlerde meydana gelen ve dünya genelinde çok önemli etkileri görülen muhasebe ve denetim hileleri, 2008 yılı sonrasında dünyada pek çok şirketin darboğaza girmesi gibi olumsuz mali sonuçlar doğurmuştur. Buna bağlı olarak, düzenleyici kurum ve kuruluşlar, paydaşların haklarının korunması ve dünya genelinde oluşan olumsuz algıyı ve etkiyi ortadan kaldırmak üzere ayrıntılı ve etkin bir risk yönetim üzerinde çalışmaya başlamışlardır. Bu yönüyle bakıldığında kurumsal yönetim işletmelerde daha çok önem kazanmıştır.

Kurumsal risk yönetimi ve iç denetim faaliyetlerinin birbirini tamamlayıcı unsurlar olarak işletmelerde uygulanmaya başlanması sonucunda iç denetimin; kurumsal risk yönetimini de kapsayacak şekilde uygulanması, artan güven ihtiyacının karşılanmasında önemli hale gelmiştir.

İç Denetçiler Enstitüsü (IIA) iç denetim ile risk yönetiminin bir bütün olarak faaliyet göstermelerinin risklere karşı daha etkili bir işletme stratejisi oluşturacağını savunmaktadır. (The Institute of Internal Auditors, 2012:3-4).

İç denetim, kurum ya da işletmede tüm faaliyet ve işlemlerin(uygulamaların), etkin ve verimli yürütülüp yürütülmediği ile ilgilidir. İç kontrol; mali tabloların güvenilirliği, uygulamaların etkinlik ve verimliliği, yürürlükteki yasa ve diğer düzenlemelere, işletme politikalarına uyum ile ilgili olarak işletme/kurum hedeflerine erişim hakkında makul güvence sağlamak amacıyla uygulanan bir süreçtir. İç denetim işletmede; kurumsal yönetim, iç kontrol ve risk yönetimi faaliyetlerinin planlandığı şekilde etkin ve verimli uygulanıp uygulanmadığını ortaya çıkarmak, varsa risklere karşı alınacak önlemlerin geliştirilmesini sağlamak amacı ile yapılan bir güvence sağlama ve danışmanlık faaliyetidir. Etkin iç kontrol önlemleri, işletme içindeki risklere odaklanarak, her türlü hata, hile ve yolsuzlukları önlemede etkili olduğu gibi yetkilendirme, bilgi güvenliği ve raporlama konularında oluşabilecek risklere karşı koruma sağlamaktadır. Bütün bunları görebilmek ancak risk odaklı iç denetim ile mümkün olmaktadır.

Günümüzdeki iç denetim, klasik anlamdaki kontrol odaklı yaklaşımdan; risk yönetimi, kurumsal yönetim ve değer katmayı esas alan, risk odaklı yaklaşıma doğru yönelmiştir. Artık iç denetçiler yalnızca kontrol faaliyetlerini denetlememekte, aynı zamanda risk evresini tanımlayarak, işletmenin risk durumunu sürekli izleyerek, risk yönetim süreçlerini desteklemektedirler (Lindow & Race, 2002:28-29).

Bu çalışmada iç kontrol alanındaki dünya çapında kabul görmüş Committee of Sponsoring Organizations (COSO) ve İç Denetçiler Birliği (IIA) yayın, yönetmelik ve uygulamaları başta olmak üzere bir literatür taraması yapılmış ve risk odaklı iç denetim ile ilgili kavram ve uygulamalar açıklanmaya çalışılmıştır.

2. İÇ DENETİMLE İLGİLİ TEMEL BİLGİLER

2.1. İç Denetimin Tanımı ve Önemi

Dünya genelinde iktisadi faaliyetlerin hızlı bir ivme kazanması ile ortaya çıkan rekabetle başa çıkmak için işletmeler yüksek kaliteli, düşük maliyetli ürünler üretmek kadar risk yönetimi gibi faaliyetlere de önem vermeye başladılar. Kurumsallaşmanın ve işletmeleri hedeflerine taşımanın önündeki riskleri ortadan kaldırmak ya da azaltmak amacı ile ortaya çıkan risk yönetimi işletmedeki bütün süreçler üzerinde de etkisini göstermektedir. İşletmelerin karar alma/ve uygulama süreçlerinde ihtiyaç duyulan bilginin zamanında, tam ve doğru bir şekilde gerekli mercilere ulaştırılması işletmelerin hedeflerini gerçekleştirebilmeleri için vazgeçilmez bir gerekliliktir. Bu bağlamda, iç denetim, işletme içi güvence hizmetleri bağlamında işletme yöneticilerinin işletme hedeflerini gerçekleştirmek için ihtiyaç duydukları makul güvenceyi sağlamaya yönelik girişimlerin başında gelmektedir (Ramamoorti, 2003:9-10).

Hem bağımsız denetim hem de iç denetime olan ihtiyaç, kar amacı gütmeyen kuruluşlarda veya ticari işletmelerde, kayıt hataları, varlıkların yanlış değerlenmesi ve hile gibi risklerin en aza indirilebilmesini sağlayacak bağımsız bir doğrulamaya duyulan gereksinimden kaynaklanmaktadır (Ramamoorti, 2003:5-8).

İç Denetçiler Birliği (IIA) iç denetimi; bir işletmede faaliyetleri geliştirmek onlara değer katmak amacıyla yürütülen bağımsız, tarafsız bir güvence ve danışmanlık faaliyeti olarak tanımlamıştır. İç denetim faaliyetleri işletmedeki risk yönetiminin değerlendirilmesi, etkinlik ve verimliliğinin arttırılması amacıyla sistematik ve disiplinli bir yaklaşımla işletmenin hedeflerine ulaşmasına katkıda bulunur (The Institute of Internal Auditors, 2008:3-6)

2.2. İç Denetimin Tarihçesi ve Ortaya Çıkış Nedenleri

Genel olarak denetimin ortaya çıkış tarihi milattan önceki yıllara kadar dayanmaktadır. Avrupa'da denetim uygulamalarına yönelik ilk bulgulara antik Roma'da rastlanmıştır ve hileli girişimleri önlemek amacıyla yapılan ticari faaliyetlerin kayıtlarının doğrulanmasına yönelik çalışmalar ilk denetim çalışmaları olarak ortaya çıkmıştır. Geriye dönük olarak incelendiğinde, denetimin ortaya çıkmasının başlıca nedeninin, hata ve hile yoluyla işletmeler tarafından elde edilen vergi avantajlarının önüne geçmek olduğu anlaşılmaktadır.

İç denetimin tarihine bakıldığında; günümüzde uygulanan iç denetimin; kurumsallaşma ve bağımsız denetimde yaşanan gelişmelerin bir gereği olarak 19.yüzyılda ortaya çıktığı görülmektedir (Spraakman, 2001:19-41). İlk iç denetim çalışmaları ABD ve Birleşik Krallıktaki demir yolu işletmelerinde görülmüştür. Bunun nedeni, coğrafi olarak birbirinden çok uzak bölgelerde faaliyet gösteren demir yolu şirketlerinin faaliyetlerini kontrol etme ihtiyacıdır. Demiryolu şirketlerinin faaliyet gösterdikleri coğrafi alanlar

genişledikçe ve mali işlemleri arttıkça, işletmelerde bağımsız bir denetim birimin bu mali işlemleri denetleme zorunluluğu doğmuştur (Ramamoorti, 2003:3-4).

Bağımsız denetimin 1930'larda ABD'de işletme hisselerinin sermaye piyasasında işlem görebilmesinin ön koşulu olarak, mali tabloların bağımsız denetimden geçmiş olması şartı getirilmiştir. Bu yaklaşım işletmelerin bağımsız denetimden önce kendi içlerinde bir doğrulama yapması ihtiyacını doğurmuş ve iç denetim uygulamaları zaman içinde değişen ve gelişen işletme yapılarına uyum sağlayarak değişmeye devam etmiştir (Ramamoorti, 2003:14-15).

İç denetimin uygulamaya başlandığı ilk yıllarda ilgi alanlarının muhasebe ve mali konularla sınırlı olduğu görülmektedir. 1978 yılında İç Denetçiler Birliği'nin onayladığı yeni tanımla birlikte iç denetimin alanı iç kontrollerin ve işletme faaliyetlerinin denetimini de kapsayacak şekilde genişletilmiştir (Anderson, 2003:97-113).

Bugünkü anlamda modern iç denetimin (risk odaklı iç denetimin) gelişim süreci aşağıdaki şekilde ifade edilebilir (Uzun, 2007:22-24). 1950'li yıllarda varlıkların korunması,

- 1960'lı yıllarda işletme bilgilerinin güvenilirliğinin sağlanması,
- 1970'li yıllarda uygunluk denetimi,
- 1980'li yıllarda işletme etkinliğinin (performans) denetlenmesi
- 1990'lı yıllarda işletme amaçlarına ulaşılmasının denetlenmesi
- 2000'li yıllarda ise risk odaklı denetimlerin gerçekleştirilmesi.

1980'li yıllara kadar iç denetim kontrol odaklı olarak uygulanmıştır. Kontrol odaklı denetim sürecinde; işletme varlıklarının korunup korunmadığı, mali tabloların ve muhasebe bilgilerinin doğru ve güvenilir olup olmadığı, işletme politikalarına yasa ve diğer düzenlemelere uygunluğun sağlanıp sağlanmadığı konuları, iç denetimin içeriğini oluşturmuştur. Bu yaklaşım geleneksel iç denetim yaklaşımı olarak ifade edilmektedir.

1980'li yıllardan itibaren iç denetim çalışmaları; faaliyetlerin etkinlik ve verimliliğinin incelenmesi suretiyle işletmeye değer katma görevini üstlenmiştir. Özellikle Enron, Parmalat vb. olaylarında etkisiyle iç denetim çalışmaları çok büyük oranda işletmelerdeki riskleri önleme ve ortaya çıkarmaya odaklanılması gereğini ortaya çıkarmıştır.

2.3. İç Denetimin Türleri

İç denetim bağımsız bir güvence ve danışmanlık hizmeti olarak (The Institute of Internal Auditors, 2008:3-6). Bir işletmede faaliyet gösteren iç denetim birimi birçok farklı hizmet sunabilmektedir. Temel olarak iç denetimin sunduğu hizmetler; güvence ve danışmanlık hizmetleri olarak iki ana başlık altında açıklanabilir. Mali denetim, etkinlik ve verimlilik denetimi, sistem denetimi gibi güvence hizmetlerinin yanı sıra; kontrollerin geliştirilmesi gibi konularda üst yönetime danışmanlık hizmeti verilmesi de iç denetimin hizmet kapsamına girmektedir (Anderson, 2003:97-113).

İç denetimin sağladığı güvence hizmetleri geleneksel iç denetim faaliyetleridir. Güvence hizmetleri genel olarak mali raporlama, faaliyet, iç kontrollerin etkinlik ve verimliliği ile risk yönetim süreçlerindeki etkinlik ve verimliliğinin denetlenmesi faaliyetlerini içermektedir (Albrecht, 2007:2-8).

Güvence hizmetleri geleneksel iç denetim faaliyetlerinden olmakla birlikte danışmanlık hizmetleri iç denetimin gelişimiyle birlikte iç denetimin faaliyetleri arasına girmiştir. Danışmanlık hizmetleri özellikle işletmenin yeni bir faaliyet alanına girmesi veya değişen işkolu ya da iktisadi koşullara uyum sağlamak amacıyla yapılacak değişikliklerin, işletme risk yönetiminde meydana getireceği muhtemel etkileri ile ilgili yönetim tarafından yapılan değerlendirmelerden oluşmaktadır (Anderson, 2003:97-113).

2.4. İç Denetimin İşletmelere Sağladığı Yararlar

İç denetim; genel olarak bir işletmede mevcut risklerin değerlendirilmesi suretiyle işletmede etkinlik ve verimliliğin artırılmasını ve bu yolla işletmeye değer katmayı hedefleyen işletme içi denetim faaliyetleridir. Bir işletmede üst yönetim; risk yönetimi, iç kontrol gibi faaliyetler ile işletmenin belirlediği hedeflerine ulaşabilmesi bakımından etkinlik ve verimliliğin kalitesini arttırabilmek amacıyla genel olarak aşağıdaki değerlendirmelerde bulunur (The Institute of Internal Auditors, 2013:2-3);

- İşletmenin stratejik hedeflerine ulaşmasında maruz kalabileceği risklerin değerlendirilmesi,
- İşletmede karar almada/vermede kullanılan bilginin ve bilgi üretim süreçlerinin tamlık ve doğruluğunun değerlendirilmesi,
- İşletmede kullanılan sistemlerin işletme politika ve planları ile kanun ve yönetmeliklere olan uyumunun değerlendirilmesi,
- Varlıkların korunması amacı ile yürütülen kontrollerin değerlendirilmesi,
- Kullanılan kaynakların etkinlik ve verimliliğinin değerlendirilmesi,
- Faaliyet ve programların; tasarlandıkları şekilde işletme amaçlarına uygun yürütülüp yürütülmediğinin değerlendirilmesi,
- İdari süreçlerin izlenmesi ve değerlendirilmesi,
- Bağımsız denetçilerin denetim faaliyetlerinin etkinliğinin ve bu faaliyetlerin iç denetim ile uyumunun değerlendirilmesi,
- İşletme yönetiminin, risk yönetimi ve kontroller konusunda danışmanlık sağlanması,
- İç denetimin amacı, sorumlulukları ve iç denetim faaliyetlerinin etkinlik ve verimliliğine ilişkin periyodik değerlendirmeler yapılması,
- İşletmenin riske maruz kalması veya hile riski ve idari düzensizlik gibi bir kontrol zafiyeti bulunması halinde konunun ilgili kurullara rapor edilmesi.

2.5. İç Denetçi ve Nitelikleri

Denetim faaliyetlerinin amacına ulaşabilmesi bakımından bağımsız bir şekilde yürütülmesi esastır. Bu nedenle iç denetim esasında işletme içi bir faaliyet olmasına karşın denetim konusunun seçimi, denetimin kapsamı, sıklığı ve zamanlaması veya denetim tekniklerinin seçimi gibi konular bakımından tamamen bağımsız olmalıdır. İç denetçiler; denetimini yaptıkları hiç bir faaliyetin icrasında (yürütülmesinde) bizzat bulunamazlar veya yürütülmesinde bulundukları hiç bir faaliyeti denetleyemezler.

Bir faaliyet veya sürecin denetiminde denetim kanıtlarının toplanması, değerlendirilmesi ve gerekli yönetim organlarına bilgi verilmesi gibi her türlü konuda iç denetçi meslek ahlakı ve profesyonellik gereklerine uygun hareket etmelidir (The Institute of Internal Auditors, 2013b:1-2).

3. İŞLETMELERDE İÇ KONTROL YAPISI

İç denetim işletme içi bir güvence ve danışmanlık hizmetidir ve en basit ifadeyle işletmede tüm faaliyet ve işlemlerin olması gerektiği gibi yürütülüp yürütülmediği ile ilgilidir. Bununla birlikte; işletme içindeki risklere odaklanan ve işletmeyi her türlü hata, hile, yetkilendirme, raporlama ve bilgi işlem gibi konularda meydana gelebilecek sorunlara karşı koruyacak bir yapı olan etkin bir iç kontrol ise, iç denetimin amacına ulaşmasını sağlayan başlıca destek unsuru olarak algılanmaktadır.

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

COSO, iç kontrolü; faaliyetlerin etkinlik ve verimliliği, mali raporların güvenilirliği, yürürlükteki kanun ve mevzuata uygunluk olmak üzere üç temel amacı gerçekleştirmeye yönelik olarak kurulan bir yapı olarak ifade edilmiştir(COSO, 2013:2-3).

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 yapı olarak ifade edilebilir (COSO, 2013:2-3).

İç kontrolün bileşenleri; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ve izleme olarak belirlenmiştir. Bu model, İç Kontrol- Bütünleşik Çerçeve (Internal Control-Integrated Framework) adı altında yayımlanmıştır (COSO, 2013:4-5).

Şirketlerde kurumsallaşma yapılarının ve maruz kaldıkları risk türlerinin değişmesi, iş ve çalışma ortamlarındaki değişiklikler, pazarlama ve faaliyetlerle ilgili olarak gelişen teknoloji ve küresel değişiklikler, hile ve yolsuzlukların tespit edilerek önlenebilmesi ile ilgili beklentiler, değişen yasalar ve mevzuata uyum sağlanması ve işletmelerin iç kontrol yapısını

güncel tutmak amacıyla COSO iç kontrol yapısına ilişkin çalışmalarını düzenli olarak güncellemeyi sürdürmektedir.

İç kontrolün nitelikleri şöyle açıklanabilir (COSO, 2011:1-5):

- 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
- İşletmelerin özelliklerine göre uyarlanabilir.

3.1. Kontrol Ortamı

İç kontrol yapısının temel bileşenlerinden biri olan kontrol ortamı; bir şirketin geçmişi, benimsediği meslek ahlak değerleri, yönetici ve çalışanların dürüstlüğü, faaliyet gösterdiği piyasa, rekabet koşulları ve yasal düzenlemeler gibi çeşitli iç ve dış faktörlerden etkilenir. Kontrol ortamının unsurları olan ilkeler; 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, bir işletmede iç kontrol yapısının yürütülebilmesi ve işletme hedeflerine ulaşılabilmesi için temel sağlamaktadır (COSO, 2011:25-50).

3.2. Risk Değerlendirme

Her işletme iç veya dış kaynaklardan gelebilecek birçok riskle karşı karşıyadır. İşletmeler açısından risk; gerçekleşmesi halinde; işletmeyi, hedeflerine ulaşması bakımından olumsuz etkiyebilecek bir olay veya olaylar olarak tanımlanabilir (COSO, 2011:51-74).

COSO'nun iç kontrol bileşenleri içinde risk değerlendirme faaliyetlerine yönelik ilkeleri ise; hedeflerin belirlenmesi, risklerin tanımlanması/belirlenmesi ve değerlendirilmesi, risklere cevap verilmesi ve değişimlerin izlenmesidir.

3.3. Kontrol Faaliyetleri

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 olmalıdır (COSO, 2011:75-90).

COSO'nun iç kontrol bileşenleri içinde kontrol faaliyetlerine yönelik ilkeleri ise; kontrol faaliyetlerinin seçilmesi ve uygulamaya konulması, teknoloji tabanlı genel

kontrollerin uygulamaya konulması, politika ve süreçlerin geliştirilmesidir**.** Yetkilendirme, onay verme, 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 ((COSO, 2013:4-5).

3.4. Bilgi ve İletişim

Etkin bir iç kontrol yapısı için; kaliteli, zamanında, ulaşılabilir, yetkisiz erişim engellenmiş(korumalı) ve doğrulanabilir bilginin sağlanması, özellikle bilgi sistemlerinin karmaşık otomasyon yapılarına sahip olduğu günümüz işletmeleri için esastır.

Gerekli bilginin zamanında doğru ve gerçek olarak 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 (COSO, 2011:91-106).

COSO'nun iç kontrol bileşenleri içinde bilgi ve iletişim faaliyetlerine yönelik ilkeleri ise; bilginin değerlendirilmesi, işletme içi iletişim süreçleri ve işletme dışı iletişim süreçleridir (COSO, 2013).

3.5. İzleme

İzleme faaliyetleri, planlanan ile gerçekleştirilenin, düzenli olarak karşılaştırılmasıdır. 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.

COSO'nun iç kontrol bileşenleri içinde izleme faaliyetlerine yönelik ilkeleri ise; sürekli izleme faaliyetleri ve gerektiğinde tesis edilen izleme faaliyetleri, eksikliklerin değerlendirilmesi ve ilgili birim ve kişilere iletilmesidir (COSO, 2011:107-118).

4. İÇ DENETİM VE KURUMSAL RİSK YÖNETİMİ İLİŞKİSİ

Günümüz işletmelerinde güçlü bir kurumsal yönetim yapısının risk yönetiminde ne denli önemli olduğu giderek daha iyi görülmektedir. Sosyal, meslek ahlakı, çevresel faktörler kadar mali ve faaliyetlere yönelik risklerin tespit edilmesi ve bu risklere karşılık verilmesi işletme faaliyetlerinin başarılı bir şekilde sürdürülebilirliğinin ve yatırımcı güveninin sağlanması açısından esastır (The Institute of Internal Auditors, 2009:1-3).

4.1. Risk Yönetimi

Kurumsal risk yönetimi, kurum ya da işletmenin amaç ve hedeflerine ulaşılması bakımından makul güvence sağlamaya yönelik bir yönetim aracıdır. Bu bağlamda; kurum ya da işletmelerin çalışmalarını stratejik plan ve performans programı hazırlık çalışmaları ile eş zamanlı olarak yürütmeleri gerekir. İşletmeler öncelikle stratejik planda gösterilen amaçları gerçekleştirmeyi sağlayacak hedefler ile riskler arasında bir denge kurarlar ve belirlenmiş olan risk iştahları çerçevesinde hedeflerini belirlerler.

Makul güvence; bir bütün olarak mali tabloların nitelik ve nicelik bakımından önemli yanlışlık (risk) içermediğine dair bir sonuca varmada, yeterli ve uygun denetim kanıtlarının toplanmasıdır. Yeterli fakat abartılı olmayan bir güvence düzeyidir (Sermaye Piyasası Kurulu, 2006)

Risk İştahı; kurum ya da işletmenin stratejik hedeflerini gerçekleştirirken almayı düşündüğü (alabileceği) risk düzeyi göstergesidir. Yönetim saldırgan ve yüksek riskli bir politika mı, yoksa hedeflere ulaşma aşamasında aşılmaması gereken sınırlamaları olan bir politika mı belirleyeceğine karar vermelidir.

Risk; "Kurum ya da işletmenin amaç ve hedeflerine ulaşmasına ve görevlerin ifasına engel olabilecek veya belirlenmeyen zararlara (sonuçlara) yol açabilecek durum ya da olaylar" şeklinde ifade edilebilir (İç Denetim Koordinasyon Kurulu, 2013:14-18)

Risk yönetimi' 'risklerin tanımlanması, değerlendirilmesi ve etkisinin kabul edilebilir bir seviyede tutulabilmesi için gerekli kontrollerin uygulanması, gözden geçirilmesi ve raporlanmasını sağlayan bir yönetim sürecidir" (İç Denetim Koordinasyon Kurulu, 2013:14-18).

4.1.1. İşletme Faaliyetlerinde Risk Türleri

İşletmeler faaliyetlerini sürdürürken birçok farklı olay, fırsat veya risk unsuru olabilmektedir. 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 (artan) risk türüdür (Beasley, 2007: 14-38).

4.1.2. Risklere Karşılık Verilmesi

Risklere karşılık (cevap) verilmesi; işletmeler (denetimlerinde) tespit edilen ve risk iştahları çerçevesinde değerlendirilen risklere verilecek cevapların ne olacağının belirlenmesi ve bu bağlamda belirlenen tehditlerin azaltılması ve/veya ortaya çıkacak fırsatların değerlendirilmesidir (COSO, 2004: 55-62).

İşletmelerin risklere cevap verme yöntemlerini belirlemeden önce mutlaka fayda-maliyet incelemesini yapmaları gerekir. Riske cevap vermede temel olarak dört yöntem kullanılmaktadır. Bu yöntemler; kabul etmek, azaltmak suretiyle kontrol etmek, devretmek ve kaçınmak şeklinde belirlenmiştir (COSO, 2004: 55-62).

Riski kabul etmek; yönetimlerin üstlenmeyi daha uygun buldukları bir cevap yöntemidir. Aşağıdaki durumlar için riskler kabul edilebilir(COSO, 2004: 55-62);

- Doğal risk, risk iştahı içinde kalıyorsa,
- Alınacak önlemlerden (kontrol etmek, devretmek veya kaçınmak) sağlanacak faydanın, alınacak önlemlerin maliyetinden daha düşük olduğunun anlaşılması durumunda,
- Bazı riskler yönetimin kontrolü dışındadır. Bazı riskler ise faaliyet sonlandırılmadıkça ortadan kalkmaz. Dolayısıyla faaliyeti her zaman sonlandırmak mümkün değildir ya da istenmez bu durumlarda risk kabul edilir.

Kontrol etmek; risklerin kabul edilebilir bir seviyede tutulması bakımından kontrol faaliyetleri aracılığı ile riske cevap verme yöntemidir. Bu yöntem aşağıdaki kontrol yöntemleri vasıtası ile uygulanır:

- Yönlendirici Kontroller: Örneğin verinin doğru bir şekilde aktarılabilmesi için yeni sistem geliştirme üzerinde çalışan Bilişim Teknolojileri (BT) personeline yeterli nitelik ve deneyimin kazandırılmalıdır.
- Önleyici Kontroller: Aktarım sırasında verinin bozulmadığından emin olmak için sistemi kabul etmeden önce BT sistemi üzerinde test yapmalıdır.
- Tespit Edici (Belirleyici) Kontroller: Yeni sistemi işletmeye başladıktan bir süre sonra, eski sistemden yeni sisteme aktarılan sürekli verilerin doğru olup olmadığını anlamak için test yapmalıdır.
- Düzeltici Kontroller; Eski sistemden aktarılan veri ile yeni sistemdeki verinin karşılaştırılması sonucu hatalı veri aktarımı olduğu belirlenmişse programda gerekli değişikliği yapmalıdır.

Riski devretmek; bazı uygulamalar yoluyla işletme yönetimin karşılaşabileceği risklere karşılık verme yöntemidir. Faaliyetlerin bir kısmını uzmanlığı olan başka bir kuruma devretmek veya belirli risklerden kaynaklanabilecek zarara karşı sigorta anlaşması yapmak riskin devredilmesi açısından en yaygın örneklerdir (Beasley, 2007: 14-38). Burada dikkat edilmesi gereken husus riskin devri söz konusu olsa dahi işletme yönetiminin risk yönetimi bakımından sorumluluğunun devam ettiğidir (COSO, 2004: 55-62)

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 (Deloitte & Touche LLP, 2012:2-6)

Riskten kaçınmak riskin her ne şekilde kontrol edilirse edilsin işletmenin kabul edilebilir risk düzeyini geçmesi durumunda verilecek en uygun risk yanıtıdır. Bu bağlamda

işletme riskli faaliyetlerden veya iş anlaşmalarından vazgeçme yoluna gidebilir (COSO, 2004: 55-62).

Belirlenen bir risk, meydana gelme veya etkisi bakımından işletmenin kabul edilebilir risk sınırları içinde yer alıyorsa, işletme bu riski kabul etme yoluna gidebilir. İşletmeler 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 (AIRMIC & ALARM, 2010: 8-16).

Kabul edilebilir risk düzeyi dışında kalan riskin oluşma ve/veya etkisine karşı, riskin azaltılmasına yönelik önlemler, uygulana en yaygın risk önlemleridir. Burada riskin gerçekleşme ihtimaline karşı bir önlem almak mümkün olmasa bile etkilerini azaltmaya yönelik önlemler alınabilir. Bazı durumlarda işletmeler kendileri için risk teşkil edebilecek bir olayın gerçekleşmesi durumunda, katlanacakları maliyetleri paylaşmayı seçebilirler ve/veya belirlenen bir riskin gerçekleşme ihtimaline karşı işletmeler riskten kaçınma yoluna gidebilirler gidebilir (COSO, 2004: 55-62).

4.2. Kurumsal Risk Yönetiminde Sorumluluklar

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 destekleyici bir tutum sergilemelidir. Yönetim Kurulu; tarafsız, yönetimden bağımsız, nitelikli ve yeterli sayıda üyeye sahip olmalıdır**.** 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. Yönetim kurulu, yönetim ve işletmenin her kademesinde yetki ve sorumluların tespiti, yetkilendirme, yetkileri sınırlandırma ve sorumlu atamalarını, görevlerin ayrılığı ilkesine uygun olarak belirler (COSO, 2011: 123-134).

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 (COSO, 2013: 2-4).

4.3. Kurumsal Risk Yönetiminde İç Denetimin Görevi

Daha önce de ifade edildiği gibi iç denetim, yönetime güvence hizmeti sağlarken aynı zamanda danışmanlık hizmeti de verebilmektedir. Burada dikkat edilmesi gereken en önemli husus kurumsal risk yönetiminde karar verme yetkisi olan üst yönetimde iç denetim birimi veya yöneticisinin söz sahibi olmaması ancak tavsiyede bulunabilmesidir. Aksi takdirde iç denetçi; vereceği güvence hizmetine yönelik olarak bağımsızlığını yitirebilir.

İç denetçi risklerin tespit edilmesinden ve bu riskleri yönetime bildirmekten sorumludur. Yönetimin risklerin yönetilmesi hususunda strateji belirlemesinde ancak öneride bulunabilir ve üst yönetimin işletme ihtiyaçlarına uygun kurumsal risk yönetimi yapısını oluşturmasında destekleyici bir rol oynayabilir (Hall, 2007:5-7).

5. RİSK ODAKLI İÇ DENETİM

İşletme yöneticileri işletme amaçlarını belirledikten sonra bu amaçlara ulaşılmasında etkili olabilecek riskleri belirlemeli ve bu risklere karşı iç kontroller ve/veya gerekli diğer risk karşılıklarını geliştirerek riski işletmenin kabul edebileceği risk düzeyinde tutmaya çalışmalıdır. Riske istenilen seviye tutmak mümkün değilse yönetim kuruluna bilgi verilmelidir. Risk yönetimine ilişkin sorumluluklar iç kontrol bileşenlerinden kontrol ortamına uygun bir şekilde tesis edilmeli ve net bir biçimde anlatılmalıdır. (COSO, 2004:67-84).

Risk odaklı iç denetim bir işletmede riskin işletmenin risk iştahına uygun olarak etkin bir şekilde yönetildiğine dair verilen bir güvence hizmetidir (Griffiths, 2006:1-2). Risk odaklı iç denetim anlayışı ile iç kontrollerin uygunluk ve yeterliliğini araştırmak, riskin izlenmesinde gerekli olacak bilgileri sağlamak ve bir iş alanında veya endüstride geçerli olan en iyi uygulamaları tanımlamak mümkün olabilmektedir (Thomas, 2007:1-6).

5.1. Risk Odaklı İç Denetimin Geleneksel Denetim Anlayışından Farkı

Risk odaklı iç denetimi geleneksel iç denetimden ayıran en önemli özellik risk odaklı iç denetimin işletmeye değer katmayı ön planda tutmasıdır. Bu bağlamda risk odaklı iç denetimle birlikte iç denetimin bakış açısı geleceğe yönelik olarak değişmiş, gelecekteki olaylara odaklanarak işletmenin amaçlarına ulaşmasını engelleyebilecek her türlü risk denetimin kapsamı içine alınmıştır.

İç kontrol faaliyetlerinin planlandığı şekilde yürütüldüğünü doğrulamak, varlıkların korunduğundan emin olmak ve işletme idaresinin yürürlükteki politikalarla uyumlu olduğundan emin olmak geleneksel denetim anlayışında olduğu gibi risk odaklı iç denetimin başlıca amaçlarındandır. Her iki yaklaşımda da yapılan kontrol değerlendirmelerinin sonuçlarını ilgili yönetim kadrolarına ve denetim komitesine rapor etmek gerekmektedir. Geleneksel iç denetim anlayışı ile risk odaklı iç denetim anlayışı arasındaki fark bu amaçlara ulaşmak için kullanılan yöntemlerin kapsamıyla ilgilidir. Risk odaklı iç denetimde, denetim

işlemleri (uygulamaları) risk değerlendirme ve denetim planlama süreçleri yoluyla belirlenmektedir (Thomas, 2007:1-6).

Tablo 1. Geleneksel İç Denetim ve Risk Odaklı İç Denetim Karşılaştırması

Özellikler	Geleneksel İç Denetim	Risk Odaklı İç Denetim
İç Denetimde Odak Nokta	İç kontrol	Risk
İç Denetim	Düzeltici yaklaşım, olaylardan sonra harekete geçme, aralıklı gözetim	Önleyici yaklaşım, sürekli gözetim
İç Denetim Testleri	Kontrol odaklı	Risk odaklı
Risk Değerleme	Risk unsurları	Senaryo planlaması
İç Denetim Yöntemleri	Kontrol testlerindeki ayrıntılar eksiksiz olarak uygulanmalıdır	İşletme risklerinin sınırları geniş bir şekilde belirlenmelidir
İç Denetim Önerileri	İç kontrole yönelik olarak titiz bir şekilde fayda-maliyet etkinliği sağlanmalıdır	Risk yönetimine yönelik olarak risk çeşitlendirmesi, riskten sakınma, riskin paylaşımı ve riskin aktarılması
İşletmede İç Denetimin Rolü	Bağımsız denetim konumu	Risk yönetimi ve üst yönetimle bütünleşik konum

Kaynak: *David McNamee ve Georges Selim, Risk Management: Changing the Internal Auditor's Paradigm.*

5.2. Risk Odaklı İç Denetimin Gerekliliği

Risk odaklı iç denetimde temel amaç iç kontrol ve kurumsal risk yönetim yapılarının tasarımının doğru olup olmadığı, işletme amaçlarına uygun bir şekilde işleyip işlemediği ile ilgilenmektir. Ayrıca kurumsal risk yönetimi ve iç kontrol uygulamalarının işletmenin karşı karşıya olduğu risklerin yönetilmesinde ne denli başarılı olduğunun incelenmesi de yine risk odaklı iç denetimin konusudur.

Kurumsal risk yönetimi işletmenin karşı karşıya olduğu riskler üzerinde dururken, denetim komiteleri geleneksel olarak mali raporlama riskleri üzerinde durmaktadır. Bununla birlikte değişen koşullar gereği iç denetim birimleri işletme risklerine karşı geliştirilen kurumsal politikaları da değerlendirmekle yükümlüdür. Risk değerlendirmesi, iç kontrol yapısının bir parçasıdır. Bu nedenle; iç denetimin görevlerinden belki de en önemlisi iç kontrollerin etkinlik ve verimliliğinin değerlendirilmesi olduğuna göre; iç denetimin risk odaklı bir şekilde yürütülmesi zorunluluğu doğmaktadır (Protiviti Independent Risk

Consulting, 2006: 40-42). Başka bir anlatımla iç denetim riskli alanlara daha çok zaman ayırmalı ve gerekli karşılıkları tespit etmede yol göstermelidir.

İşletmelerde görevli iç denetim birimleri üst yönetimle birlikte risk değerlendirmesi yapmakla yükümlüdür. Burada yapılacak risk değerlendirmesi esasen iç kontrol süreçlerinde belirlenen risklere karşı işletmenin ne derecede başarı ile karşılık verebildiğinin değerlendirmesidir.

Gelecekte meydana gelebilecek ve işletmeyi ciddi biçimde etkileyebilecek olayların tanınması, tartışılması, bu olayların değerlendirilmesi, risklerin belirlenmesi ve belirlenen risklerin ne ölçüde kabul edileceğine karar verilmesi, kabul edilmeyecek risklere karşı önlemler ve kontroller geliştirilmesi yönetimin görevidir (COSO, 2004). Bununla birlikte bu süreçlerin tamamının tasarlandığı şekilde yürütüldüğünden emin olmak için iç denetimin risk odaklı bir şekilde değerlendirmelerde bulunması gerekmektedir.

5.3. Risk Odaklı İç Denetimin İşleyişi

Risk odaklı bir iç denetim yaklaşımında geleneksel bir iç denetim yaklaşımından farklı olarak risklerin başarılı bir şekilde yönetilmesine büyük önem verilir. Bu yaklaşımda ilk olarak işletme yönetiminin gerçekçi, ulaşılabilir hedefler belirleyip belirlemediği incelenir. Sonrasında yönetimin bu amaçlara ulaşırken işletmenin karşılaşabileceği riskleri ne ölçüde değerlendirdiğine bakılır. Yönetimin belirlediği riskler iç denetim birimi için yeterli olmamalıdır. İç denetim birimi yönetimden bağımsız olarak kendi içinde de bir risk belirlemesi yapmalıdır (The Institute of Internal Auditors – UK and Ireland, 2003:1-4).

İç kontrol yapısı bakımından risk odaklı iç denetim anlayışında iç kontrolün tasarımından uygulanmasına kadar tüm aşamaların etkinlik ve verimliliği değerlendirilmelidir. İç kontrolün her bir bileşeni ve bu bileşenlere ilişkin her bir aşama iç denetimin kapsamına dâhil edilmelidir.

Kurumsal risk yönetimi açısından iç denetimin görevi, işletme yönetiminin uygun risk politikaları geliştirip geliştirmediğini denetlemek ve bu konuda üst yönetim ve yönetim kuruluna makul güvence vermektir. Ayrıca iç denetim birimi uygun risk yönetim politikalarının geliştirilmesi hususunda; gerektiğinde yönetime danışmanlık hizmeti sunmalı ve yol gösterici bir tutum izlemelidir.

5.4. Risk Odaklı İç Denetim Süreci

İç Denetçiler Birliği'nin bir yayınında risk odaklı iç denetim için yedi adımlık bir süreçler dizisi önermektedir. Bunlar sırasıyla; (1) işletme çevresini anlamak, (2) ön risk değerlendirmesi yapmak, (3) 3 yıllık bir denetim planı geliştirmek, (4) ikinci risk değerlendirmesini tamamlamak, (5) iç denetim planının icra etmek, (6) kapanış toplantısı yapmak ve (7) raporlama ve iletişim süreçleri oluşturmak (Thomas, 2007:1-6).

5.4.1. İşletme Çevresini Anlamak (Tanımak)

Etkin bir risk odaklı iç denetim için ilk adım, iç kontrol dâhil işletmeyi, işletmenin çevresini ve iş süreçlerini anlamaktır. Bu aşamada işletme amaçları incelenir. Yönetimin bu amaçlara ulaşmasında engel teşkil edebilecek riskler tanımlanır ve bu risklere karşı geliştirilmiş kontrollerin etkinliği değerlendirilir.

5.4.2. Ön Risk Değerlendirmesi

Ön risk değerlendirmesinin amacı işletmedeki risk düzeyini ve her bir iş (faaliyet) birimindeki süreçlere yönelik kontrollerin uygunluğunu belirlemektir. İşletmenin ticari profili, yönetim yapısı, örgütsel değişiklikler, yönetim ve denetim komitesi değişiklikleri gibi alanlar ön değerlendirmelere konu olan başlıca alanlardır. Bu alanlarda yapılan incelemeler neticesinde işletme süreçlerinde riskli alanlara göre derecelendirmesi yapılabilir.

5.4.3. Yıllık Denetim Planı

Ön risk değerlendirmesinde işletme süreçleri ve öncelikli alanlarda yapılan risk analizleri ve risk derecelendirmesi yapıldıktan sonra, denetim planı hazırlama aşamasına geçilebilir. Riskin önem derecesine göre; az riskli alanların üç yılda bir, orta derecede riskli alanların iki yılda bir ve yüksek derecede riskli alanların ise her yıl denetiminin yapılmasının uygun olduğu kabul edilir. Denetim planı; her yıl yapılan risk değerlendirmelerinin sonuçlarına göre güncellenmeli ve varsa değişikliklere uygun olarak yeniden tasarlanmalı ve geliştirilmelidir.

5.4.4. İkinci Risk Değerlendirmesi

İkinci risk değerlendirmesinde belirlenen risklere karşı işletmenin geliştirdiği kontrollerin etkinliği analiz edilir. Bu aşamada iç denetçi mülakatlar (sorular sorarak), yerinde denetimler gibi teknikler kullanarak yönetim tarafından faaliyete geçirilmiş kontrollerin gerçekte tasarlandığı şekilde çalışıp çalışmadığını inceler. Ön risk değerlendirmesinde iç denetçi daha çok yönetimden aldığı bilgilere göre risk derecelendirmesi yaparken; ikinci risk değerlendirmesinde kontrolleri bizzat test eder ve kesin bir risk derecelendirmesi yapar. Denetim planı ikinci risk değerlendirmesinden elde edilen sonuçlara göre daha da geliştirilir son şeklini alır.

5.4.5. İç Denetim Planın İcra Edilmesi

Denetim planında gerekli değişiklikler yapıldıktan ve son şekli verildikten sonra plan tamamlanır ve denetim fiilen başlayacak aşamaya gelir. Standart bir denetim planı gereğince; ikinci risk değerlendirmesinin sonuçlarına göre uygulanacak denetim yöntem ve işlemleri belirlenir. Yüksek risk derecesine sahip alanlarda daha fazla denetim işlemleri uygulanması genel bir kabuldür.

Denetim süreci boyunca ve kapanış toplantısından önce tüm muhtemel denetim konularının gerekli personel ve yönetim kadrosuyla görüşülmesi gerekmektedir. Bu görüşmeler ile iç denetçi denetim süreci boyunca edindiği bulguların doğruluğunu değerlendirme fırsatı bulur ve gereksiz denetim çalışmaları yapılmasının da önüne geçilebilir. Ayrıca; personel ve yönetim gerekli düzeltmeleri yapmaya başlayabilir veya iç denetçi ile fikir birliğine varamadıkları konularda önceden bilgi sahibi olabilirler.

5.4.6. Kapanış Toplantısı

Kapanış toplantısı denetim sonucu sunmadan ve kontrollerin, etkinlik ve verimliliğin geliştirilmesi için öneride bulunmadan önce yapılmalıdır. Kapanış toplantısına hem orta hem de üst düzey yöneticiler katılmalıdır. Bu toplantı; denetim raporu hazırlanmadan önce iç denetçi ve yönetim arasında bilgi paylaşımı sağlaması ve fikir birliğine varılması için bir fırsat olarak görülmelidir.

5.4.7. Raporlama ve İletişim

Kapanış toplantısından sonra taslak denetim raporu hazırlanmalıdır. Raporda belirlenen riskler düzeyleri (yüksek, orta ve düşük) ile birlikte yer almalıdır. Ayrıca bu riskleri ortadan kaldırmak için önerilen çözümlere de taslak raporda yer verilmelidir. Burada risklerin dereceleri önemlidir. Yüksek risk düzeyi; yönetimin acilen önlem alması gereken alanları, orta risk düzeyi zamanında önlem alınması gereken alanları ifade ederken düşük risk düzeyi acilen önlem alınması gerekmeyen fakat kontrollerin yine de geliştirilmesi gereken alanları ifade etmektedir. Taslak rapor aşamasında iç denetçi ile yönetim arasında bulgulara yönelik bir fikir ayrılığı kalmamış olmalıdır. Taslak rapora göre yönetim bir eylem planı oluşturur ve eylem planında iç denetçi önerileri ile uygun bir şekilde belirlenen risklere karşı alınacak önlemler ve kontrolleri ne şekilde geliştirileceğine yer verilir.

Nihai denetim raporunda hem iç denetçinin bulgu ve önerilerine hem de yönetimin hazırladığı eylem planına yer verilir. Nihai rapor gerekli tüm orta ve üst düzey yönetim kadrolarına iletilmelidir. İç denetçi düzenli olarak denetim komitesi ile denetim raporu ve önerilerin işletmede nasıl hayata geçirildiği ile ilgili görüşmeli ve böylece düzenli bir izleme faaliyeti oluşturulmalıdır.

6. SONUÇ

Dünya genelinde işletmelerin sahiplik yapıları giderek değişmektedir. Günümüzde yatırımcılar dünyanın herhangi bir yerinde mevcut olan birçok farklı işletmede hisse sahibi olabilmektedir. Gerek iktisadi gerekse sosyal dengelerin değişmesi ve buna bağlı olarak iktisadi hayatın ve iktisadi birimlerin yeniden ve değişerek şekillenmesi birçok sorunu da beraberinde getirmektedir. Yatırımcıların ve diğer çıkar gruplarının işletmeler üzerinde tam bir kontrole sahip olamamasından kaynaklanan güven sorunu neticesinde iç denetim faaliyetlerinin gerekliliği ortaya çıkmıştır. İşletme dışı paydaşların işletme içindeki temsilcisi

rolünde olan yönetim kurulu; tüm paydaşlar adına işletme faaliyetlerine yönelik makul güvence sağlamakla yükümlüdür ve bu görevi iç denetim aracılığı ile yerine getirmektedir.

Geleneksel iç denetim anlayışının başlangıç noktası vergi kaçakçılığının önüne geçmek, mali hile ve yolsuzlukları önlemektir. Zaman içinde kurumsallaşmaların artması, çokuluslu şirketlerin ortaya çıkması ve çoğalması, teknolojideki hızlı değişimler ve iktisadi hayatta sınırların ortadan kalkması gibi nedenlerle iç denetim anlayışında da birçok farklılıklar meydana gelmiştir. Günümüzde iç denetim; iç kontrol, kurumsal risk yönetimi ve kurumsal yönetim gibi yapılarla paralel bir şekilde uygulanmaktadır.

İç kontrol; bir işletmedeki tüm faaliyet ve yönetim kademelerinin etkin bir şekilde görev aldığı bir yapıdır. Temel amaçları ise faaliyetlerin etkinlik ve verimliliği, mali raporların güvenilirliği ve yürürlükteki kanun ve mevzuata uygunluğa yönelik olarak işletme yönetimine makul güvence sağlamaktır. Kurumsal risk yönetimi; işletme amaçlarına yönelik olarak karşılaşılabilecek risklerin yönetildiği bir süreçtir. İç kontrol ise işletme faaliyetlerine paralel bir şekilde yürütülen ve her bir faaliyete özgü tasarlanan kontrol faaliyetlerinden oluşurken, kurumsal risk yönetimi daha ziyada işletme hedeflerine ulaşılmasında işletmelerin karşı karşıya kalabileceği risklerin yönetilmesi ile ilgilidir.

Risk odaklı iç denetimin gelişimi iç kontrol ve kurumsal risk yönetiminin gelişimi ile paralel özellikler göstermektir. Geleneksel iç denetim anlayışında iç denetim birimine atfedilen birçok görev günümüzde iç kontrol ve kurumsal risk yönetimi uygulamaları ile yürütülmektedir. İç denetimin görevi gerek iç kontrol gerekse kurumsal yönetim uygulamalarının tasarımı ve işleyişi hakkında işletme içi güvence ve danışmanlık hizmeti sunmaktır. Risk odaklı iç denetim anlayışı; bu yapıların tasarlanması ve faaliyetlerinin işletme hedeflerine uygunluğunu inceleyerek riskli görülen alanlar için yönetime önerilerde bulunmaktır.

KAYNAKLAR

AIRMIC & ALARM (2010), ‘2*A structured approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000’’,* AIRMIC (Association of Insurance and Risk Managers), pp.8-16, http://www.airmic.com, (03.12.2014)

Albrecht, T. (2007), ‘’*What assurance to expect from Internal Audit? An external audit view’’, IAS Conference Bulletin.* Brüksel: European Comission, pp.2-8 http://ec.europa.eu, (03.12.2014)

Anderson, U. (2003). ‘’Assurance and Consulting Services’’, *Research Opportunities in Internal Auditing*,Florida, ABD, IIA, pp.97-113. https://na.theiia.org, (10 12 2014)

Beasley, M. S (2007), ‘’*Developing Effective Internal Controls Using the COSO Model’’*, Raleigh, ABD: Enterprise Risk Management Initiative, pp. 14-38, http://www.ncosc.net , (03.12.2014)

COSO (2004), ‘’*Enterprise Risk Management- Integrated Framework, Application Techniques’’*,. COSO, http://www.coso.org, (03.12.2014)

COSO (2011), ‘’*Internal Control- Integrated Framework’’* COSO, http://www.coso.org, (03.12.2014)

COSO (2013), ‘’*Internal Control — Integrated Framework. Executive Summary’’* COSO, https://na.theiia.org, (03.12.2014)

Deloitte & Touche LLP. (2012). *Risk Assessment in Practice.* COSO. http://www2.deloitte.com, (03.12.2014)

Griffiths, D. (2006), ‘’*Risk Based Internal Auditing: Three Views on Implementation’’,pp..1-2,* www.internalaudit.biz, (03.12.2014)

Hall, J. (2007), ‘’*Internal Auditing and ERM: Fitting in and Adding Value’’,* Dallas, ABD: The University of Texas at Dallas, pp..5-7

İç Denetim Koordinasyon Kurulu (2013), ‘’*Kamu İç Denetim Rehberi’’,* Ankara: İDKK, s.14-18, (http://www.idkk.gov.tr, 03.12.2014)

Lindow, P. E., & Race, J. D. (2002), ‘’Beyond Traditional Audit Techniques’’, *Journal of Accountancy*, pp.28-29.

McNamee, D., & Georges, S(1998), ‘’*Risk Management: Changing the Internal Auditor's Paradigm’’* IIA Research Foundation, pp.5-6

Protiviti Independent Risk Consulting (2006), ‘’*Guide to Enterprise Risk Management’’*, Atlanta, ABD: Protiviti Independent Risk Consulting, pp.40-42, http://www.ucop.edu, (03.12.2014)

Ramamoorti, S. (2003), ‘’*Internal Auditing: History, Evolution, and Prospects’*, IIA, https://na.theiia.org, (03.12.2014)

Ramamoorti, S. (2003d), ‘’*Internal Auditing: History, Evolution, and Prospects’*, IIA, s.14-15 (https://na.theiia.org, 03.12.2014)

Sermaye Piyasası Kurulu (2006), ‘’*Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ.Seri:X,No:22’’ (* 26196 sayılı Resmi Gazete)

Spraakman, G. (2001), ‘’*Internal audit at the historical Hudson's bay company: A challenge to accepted history’’, Accounting Historians Journal*, pp.19-41.

The Institute of Internal Auditors – UK and Ireland (2003), ‘’*Risk Based Internal Auditing’’,* IIA – UK and Ireland, pp.1-4, http://www.cqs.co.za, (03.12.2014)

The Institute of Internal Auditors (2008), ‘’*International Standards for the Professional Practice of Internal Auditing (Standards)’’,Florida, ABD: IIA, pp.3-6* https://na.theiia.org, (03.12.2014)

The Institute of Internal Auditors(2009) ‘’*The Role of Internal Auditing in Enterprise Wide Risk Management’’*, Florida, ABD, IIA, s.1-3 (https://na.theiia.org, 03.12.2014)

The Institute of Internal Auditors (2012), '2*Risk Management and Interna lAudit: Forging a Collaborative Alliance''*. Florida, ABD: IIA, pp.3-4, https://na.theiia.org, (03.12.2014)

The Institute of Internal Auditors.(2013),'' *Model Internal Audit Activity Charter''*, Florida, ABD, IIA, https://global.theiia.org, (03.12.2014)

Thomas, M. (2007), ''*The Seven-step Process to Risk-based Auditing'', FSA Times,* Florida, ABD: IIA, pp.1-6

Uzun, A. K. (2007) ''*İşletmelerde İç Denetimin Kurulması, Rolü ve Önemi''* Antalya: Deloitte, s.22-24, www.ismmmo.org.tr (03.12.2014)