T.C.

KOCAELİ ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ TEMELLİ İÇ DENETİM VE TÜRKİYE UYGULAMALARI

DOKTORA TEZİ

DAVUT PEHLİVANLI

ANABİLİM DALI : İŞLETME

PROGRAMI : MUHASEBE FİNANSMAN

KOCAELİ, 2008

T.C.
KOCAELİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ TEMELLİ İÇ DENETİM VE TÜRKİYE UYGULAMALARI

DOKTORA TEZİ

DAVUT PEHLİVANLI

ANABİLİM DALI : İŞLETME
PROGRAMI : MUHASEBE FİNANSMAN

DANIŞMAN : PROF. DR. YUNUS KİSHALI

KOCAELİ, 2008

T.C.

KOCAELİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ

KURUMSAL RİSK YÖNETİMİ TEMELLİ İÇ DENETİM VE TÜRKİYE UYGULAMALARI

DOKTORA TEZİ

Tezi Hazırlayan : DAVUT PEHLİVANLI

Tezin Kabul Edildiği Enstitü Yönetim Kurulu Tarihi ve No : 25.06.2008-2008/18

Prof. Dr. Yunus KİSHALI

Prof. Dr. Gültekin RODOPLU

Prof. Dr. Selman Aziz ERDEN

Prof. Dr. Göksel YÜCEL

Prof. Dr. Nejat BOZKURT

KOCAELİ, 2008

SUNUŞ

İç denetim; sorumlulukları ve çalışma alanı günden güne genişleyen, güvence ve danışmanlık arasındaki hassas çizgi başta çıkar çatışmaları olmak üzere pek çok faktörden etkilenen bir alanda faaliyet göstermektedir.

2000'li yıllarda yaşanan krizlerle kurumsal yönetim açısından önemi bir kez daha ortaya çıkan iç denetimin faaliyet alanına, son olarak risk yönetimi dahil edilmiştir. Risk yönetimi sürecinde güvence ve danışmanlık hizmetlerini bir arada yürüten iç denetim birimi hem objektifliğini kaybetmemeli hem de kuruma değer katmaya devam etmelidir. Bu hassas denge de sınırları çok iyi çizilmiş iç denetim yönetmeliği ve etkin çalışan denetim komitesi ile mümkün olabilecektir.

Bu çalışma ile risk yönetimi ve iç denetim arasındaki olası veri paylaşım alanları belirlenmeye çalışılmış, risk yönetimi temelli çalışan bir iç denetim sistemi tasarlanmış ve iç denetimin risk yönetimi sürecinde üstlenmesi ve üstlenmemesi gereken roller Türkiye uygulamaları açısından incelenmiştir. Çalışmanın sözkonusu açılımları sağlamasının faaliyet raporu ve kurumsal yönetim uyum raporları incelemelerine ek olarak anket çalışması ile mümkün olmayacağı görülmüştür. Buradan hareketle çalışma gerçekleştirilen mülakatlarla zenginleştirilmiş ve sözkonusu açılımlara bir nebze de olsa ulaşılmıştır.

Bu çalışmanın her aşamasında özellikle çalışmaya yön veren yurt dışı sürecinde desteğini her zaman yanımda hissettiğim değerli hocam sayın Prof. Dr. Yunus KİSHALI'ya, çalışmanın şekillenmesine katkıda bulunan Türkiye İç Denetim Enstitüsü Kurucu Başkanı sayın Ali Kamil UZUN'a, güncel meslek uygulamaları hakkında deneyimlerini paylaşan Türkiye Kurumsal Yönetim Derneği Başkanı sayın Tayfun BAYAZIT'a ve Türkiye İç Denetim Enstitüsü Başkanlarından sayın Özlem AYKAÇ'a son olarak da bilgiyi paylaşımcı tutumları ve çalışmanın mülakat kısmına olan katkılarından dolayı KPMG firması yetkilileri sayın Ebru YARDIMCI ve Sezer Bozkuş KAHYAOĞLU'na teşekkürü bir borç bilirim.

Umuttepe, Haziran 2008 Davut PEHLİVANLI

İÇİNDEKİLER

II. BÖLÜM

KURUMSAL RİSK YÖNETİMİ

III. BÖLÜM

KURUMSAL RİSK YÖNETİMİ TEMELLİ İÇ DENETİM FAALİYETİNİN PLANLANMASI, YÜRÜTÜLMESİ VE RAPORLANMASI

IV. BÖLÜM

RAPOR İNCELEMELERİ, RİSK YÖNETİMİ TEMELLİ İÇ DENETİM İMKB ANKET UYGULAMASI VE MÜLAKAT ÇALIŞMASI

ÖZET

İşletmelerin farklılaşan ihtiyaçları, iç denetimde odak noktanın zaman içinde değişmesine neden olmuştur. Kontrollere ilave olarak önce kurumsal yönetim ardından da risk yönetimi iç denetimin faaliyet alanına girmiştir. İç denetim biriminin risk yönetimi sürecindeki olası rolleri bu çalışmanın temelini oluşturmaktadır.

Kurumsal Risk Yönetimi (KRY) Temelli İç Denetim şeklinde ifade edilebilecek olan bu yaklaşım, çalışmada COSO tarafından yayınlanan KRY çerçevesi temel alınarak tasarlanmıştır. Bu yaklaşım, KRY sürecinden denetime veri transferini mümkün kılmaktadır.

Çalışmanın 1. bölümünde iç denetim ve kurumsal yönetim ayrıca denetim açısından riskler ve Türk mevzuatı açısından durum ele alınmaktadır. 2. bölümde, kurumsal risk yönetimi ve araçları incelenmektedir. Çalışmanın 3. bölümünde ise kurumsal risk yönetimi ve iç denetimin paralel çalışabileceği düşüncesinden hareketle bu iki süreç bütünleştirilmekte ve kurumsal risk yönetimi temelli iç denetimin planlanması, yürütülmesi ve raporlanması aşamaları inlenmektedir. Çalışmanın son bölümü ise faaliyet ve kurumsal yönetim raporu incelemelerine, anket çalışmasına ve gerçekleştirilen mülakatların değerlendirilmesine ayrılmıştır.

Çalışma sonuçları itibariyle, Türkiye'de iç denetim birimlerinin KRY sürecinde görev aldığını ve bu sürece yönelik güvence ve danışmanlık hizmetleri verdiğini göstermektedir. Fakat uluslararası uygulamaya kıyasla kurumsal düzeyde iç denetim alanında önemli uygulama eksiklikleri olduğu tartışılmaz bir gerçektir.

ABSTRACT

Ever-changing scope of corporate management has given rise to the transformation of the focal point of internal-auditing over the course of the recent decades. In addition to the controls, the corporate governance and risk management have respectively became a subject matter of the internal-auditing. Potential roles of the internal-auditing in the process of risk management constitute the main subject matter of this study.

Articulated as 'Enterprise Risk Management (ERM) Based Internal Auditing', this approach, in this dissertation, is conceptualized under the guidance of the ERM framework published by COSO. The approach makes it possible to transfer data from the process of ERM to auditing.

In the first section of the study, internal auditing and corporate governance along with the risks from auditing perspective and the situation in Turkish legislation is analysed. The second section explores enterprise risk management, and tools of enterprise risk management. As for the third part of the study, it conflates enterprise risk management with internal auditing in regard to the fact that they can accommodate, and then deals with planning, conducting and reporting processes of enterprise risk management based internal auditing. The final part is devoted to the analysis of annual report and corporate governance principles compliance report, survey study and interviews.

The study finds out that auditing units, in Turkey, become involved in the process of ERM, and offer assurance and consultancy services for this process. But, there is no doubt in the fact there are out striking shortcomings in practice compared to the international applications.

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

BDDK : Bankacılık Düzenleme ve Denetleme Kurulu

CEO : Chief Executive Officer

CFO : Chief Financial Officer

COSO : Committee of Sponsoring Organizations of the Treadway Commission

CoCo : Guidance on Control

CRSA : Control Risk Self Assessment

ERM : Enterprise Risk Management

FTSE : Financial Times Stock Exchange

IIA : The Institute of Internal Auditors

İMKB : İstanbul Menkul Kıymetler Borsası

KRY : Kurumsal Risk Yönetimi

KRÖD : Kontrol-Risk Öz Değerlendirme

PCAOB : Public Company Accounting Oversight Board

m : milyon

SAP : Systems Applications and Products in Data Processing

SOX : Sarbanes Oxley

SPK : Sermaye Piyasası Kurulu

SPSS : Statistical Package for Social Sciences

SWOT : The Strengths, Weaknesses, Opportunities, and Threats

TTK : Türk Ticaret Kanunu

TÜSİAD : Türkiye Sanayici ve İş Adamları Derneği

YK : Yönetim Kurulu

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

GİRİŞ

Sosyal bilimlerde olayları tek bir nedene dayandırmak veya olayları tek bir değişkenle açıklamak mümkün değildir. Sonuçları itibariyle pek çok tarafı ilgilendiren ekonomik krizlerin ortaya çıkış nedenleri farklı başlıklar altında sınıflandırılabilir. Tek başına, krize neden olmayan fakat krize götüren süreçte büyük etkisi bulunan temel faktör muhasebe kökenli bilgidir.

1930'lu yıllarda yaşanan ekonomik bunalım sermaye piyasalarında düzenleyici otorite gerekliliğini ortaya çıkarmış ve modern anlamda denetim uygulamalarına geçişi hızlandırmıştır. Denetimin olgunlaşması sürecinde kuşkusuz 1940'lı yıllarda adından söz ettirmeye başlayan iç denetim uygulamalarının da etkisi büyüktür.

1930'lardan 2000'lere kadar pek çok ekonomik kriz yaşanmış ve muhasebe denetim mesleğinde de başta uluslararası standartlar olmak üzere çok sayıda yeni uygulama evrensel ölçekte kullanılmaya başlanmıştır.

2000'li yılların başında yaşanan ENRON skandalı ile birlikte risk yönetimi uygulamaları daha çok dikkate alınır hale gelmiş ve bu süreçte iç denetim birimlerinin olası rolleri ve sorumluluk alanları çok tartışılmıştır. Özellikle reel sektör işletmeleri açısından risk yönetimi sürecinin hızlanmasına katkıda bulunan diğer bir gelişmede BASEL II prensipleri çerçevesinde işletmelerin kredi derecelendirmesinin yapılmasına olan ihtiyaçtır.

Türkiye'de yakın bir gelecekte uygulanmaya başlanması planlanan BASEL II prensipleri; risk yönetimi sisteminden gelecek verileri daha önemli hale getirmektedir. Özellikle bankacılık sisteminden kredi alacak işletmelerin kredi derecelendirmesinden geçecek olmaları bağımsız denetimin yanısıra iç denetim ve risk yönetimine olan ihtiyacı artırmıştır.

Bağımsız denetimdeki ilerlemelere paralel bir şekilde iç denetim faaliyetlerinin de odak noktası ve sektör uygulamaları gelişme göstermiştir. İç denetim yaklaşımları kontrol odaklı, süreç odaklı, risk odaklı ve risk yönetimi odaklı şeklinde sınıflandırılabilir. Bununla beraber iç denetimin odak noktasının değişmesi geleneksel iç denetim faaliyetlerinin ihmal edildiği anlamına gelmemekte tam tersi iç denetim faaliyetleri sıralanan dört farklı yaklaşımı da bünyesinde taşıyarak zenginleşmektedir.

Hangi yaklaşım ağırlıkta olursa olsun iç denetim birimi çeşitli alanlarda güvence ve/veya danışmanlık hizmetlerini yürütmektedir. Yaygın kanı ve standartlarda da kabul edildiği üzere iç denetim birimi sorumluluk üstlenmeden risk yönetimi faaliyetleri ile ilgili danışmanlık ve güvence hizmeti verebilir ve ayrıca gerekiyorsa bu faaliyetleri kısmen yürütebilir veya koordine edebilir şeklindedir.

Risk yönetiminin temelinde de iç kontrol uygulamalarının bulunduğu gerçeğinden hareketle özellikle reel sektör işletmelerinde risk yönetimi faaliyetlerinin çeşitli aşamalarının iç denetim birimi tarafından yürütülmesi kaynakların etkin kullanımı açısından optimum bir yapılanmadır. Kuşkusuz bütün olarak risk yönetimi faaliyetini üst yönetim yürütmelidir.

Sözkonusu bu görev dağılımı ve işletmelerin organizasyon yapılarına yansımaları kurumsal yönetim ilkeleri çerçevesinde olmalıdır. Bu faaliyetlerin etkinliklerini maksimize edici diğer yandan benzer nitelikteki işlemlerin farklı birimler tarafından tekrar edilmesini önleyici bir örgüt yapısı kaynakların etkin kullanımı açısından temel şarttır.

Kurumsal yönetim ilkelerinin de temel amacı olan hak sahiplerinin doğru, tam ve zamanında bilgilendirilmesi başta bağımsız denetim olmak üzere iç denetim ve risk yönetimi sistemlerinin etkin işlemesine bağlıdır.

İşletmelerin faaliyetlerinin izlenmesi ve gerekli önlemlerin alınması sürecinde bağımsız denetim, iç denetim ve risk yönetiminden oluşan üçlü bir yapılanma sözkonusudur. Bilindiği üzere bağımsız denetim, finansal tabloların gerçeğe en yakın halleriyle yayınlanması amacıyla faaliyet gösterirken iç denetim ise temelde işletmelerin hedeflerine ulaşabilmeleri için faaliyetlerini geliştirmek ve değer katmak amaçlı çalışmaktadır. İç denetim sözkonusu amaca risk yönetimi, kontroller ve

yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek için yürüttüğü güvence ve danışmanlık hizmetleri ile katkıda bulunmaktadır.

Küresel ölçekte iç denetim birimlerinin risk yönetimi sürecinde güvence ve danışmanlık hizmeti verdiği alanlar farklılık gösterebilmektedir. Bu farklılığa neden olan temel faktörler yasal mevzuat, üst yönetimin iç denetime bakış açısı, denetim komitesinin istekleri ve işletme risk yönetimi sisteminin olgunluk seviyesi olarak sıralanabilir.

İç denetim faaliyetine yön veren dahası risk yönetimi sisteminin çıktılarının iç denetimin gerek planlama gerekse de denetimin yürütülmesi ve raporlama aşamalarında kullanılması işletme risk yönetimi sisteminin olgunluk seviyesi ile paralellik göstermektedir.

Bu çerçevede çalışmanın amacı, risk yönetimi ve iç denetim faaliyetlerinin ortak paydalarını, organizasyon yapıları itibariyle üst yönetimden en alt kademe çalışanlarda dahil sorumluluk alanlarını belirlemek, uygulamada risk yönetim faaliyetinin iç denetim birimleri tarafından yürütüldüğü durumları incelemek ve olası sorunlara çözüm önerileri getirmektir.

Sınırları Kurumsal Risk Yönetimi ve iç denetim uygulama olanaklarının araştırılması şeklinde çizilen çalışma giriş ve sonuç bölümleri hariç dört bölümden oluşmaktadır. Çalışmanın birinci bölümü iç denetim, riskler ve yönetimine ayrılmıştır. Bu bağlamda öncelikle iç denetimin tarihi gelişimi ve iç denetim kavramı ardından kurumsal yönetim bağlamında iç denetim, denetim açısından riskler ve yönetimi son olarak iç denetim ve risk yönetiminin Türk mevzuatı içindeki yeri ele alınmaktadır.

Çalışmanın ikinci bölümünde Kurumsal Risk Yönetimi'nin teorik çerçevesi çizilmeye çalışılmış ve uygulamadan örneklerle desteklenmiştir. Bu bölümde öncelikle geleneksel risk yönetimi yaklaşımından kurumsal risk yönetimi yaklaşımına uzanan süreç, kurumsal risk yönetimi çerçevesi bileşenleri, kurumsal risk yönetimi araçları ve son olarak kurumsal risk yönetimi sisteminin sınırları incelenmektedir.

Çalışmanın üçüncü bölümü ise kurumsal risk yönetimi temelli iç denetim faaliyetinin planlanması, yürütülmesi ve raporlanması başlığını taşımaktadır. Bu

bölümde sırasıyla risk yönetimi temelli iç denetim ve ortaya çıkışı, risk yönetimi temelli iç denetimin aşamaları, kurum yapısının anlaşılması ve risk yönetimi olgunluğu, risk yönetimi temelli iç denetimde planlama, risk yönetimi temelli iç denetimin yürütülmesi, risk yönetimi temelli iç denetimde raporlama ve son olarak risk yönetimi temelli denetimin avantaj ve dezavantajları ele alınmaktadır.

Uygulamaya ayrılan son bölüm ise konunun geçmişi ve öneminin incelenmesiyle başlamakta, risk yönetimi temelli iç denetime ilişkin literatür taraması, çalışmanın genel amacı, çalışmanın yöntemi ve kapsamı ile devam etmektedir. Çalışmanın uygulaması; faaliyet raporu ve kurumsal yönetim uyum raporu incelemesi, anket ve mülakat çalışması şeklinde tasarlanmıştır.

I. BÖLÜM
İÇ DENETİM - RİSKLER VE YÖNETİMİ

Tarihsel süreç içinde incelendiğinde iç denetimin faaliyet alanına sırasıyla kontrollerin, kurumsal yönetimin ve son olarak da risk yönetiminin girdiği görülmektedir. Bu değişiklikler işletmelerin organizasyon yapılarına ve sonuç olarak mevzuata da yansımıştır.

1.1. İÇ DENETİMİN TARİHİ GELİŞİMİ VE İÇ DENETİM KAVRAMI

İç Denetçiler Enstitüsü'nün (The Institute of Internal Auditors – IIA) kurulmasıyla profesyonel anlamda bir meslek olarak kabul gören iç denetimin sorumluluk üstlendiği, danışmanlık ve güvence hizmetlerini yürüttüğü alanlar zamanla farklılaşmıştır. Yaşanan bu farklılaşmalar yapılan iç denetim tanımlarının sürekli güncellenmesini sağlamıştır. 1940'lı yıllarda iç denetim sadece muhasebe finansman faaliyetleri ile ilgilenmekteyken günümüzde artık bütün olarak işletmenin faaliyetleri iç denetimin faaliyet alanına girmektedir.

1.1.1. İç Denetimin Tarihi Gelişimi

Dış denetim mesleğinin geçmişi milattan önce 3000'li yıllara kadar dayandırılmakla birlikte, iç denetim mesleğinin ortaya çıkışı 1900'lü yılların başı olarak kabul görmektedir. Bununla beraber iç denetimin modern bir meslek olarak kabul görmesi 1941 yılında Amerika'da İç Denetçiler Enstitüsü'nün kurulması ile başlar[1].

Ortaya çıkış gerekçesi olan objektif bilgi sağlama fonksiyonunu yerine getiren iç denetimin, İç Denetçiler Enstitüsü'nün kurulması ile birlikte farklı tanımları yapılmış ve odak noktası sürekli değişmiş ve gelişmiştir. İç denetimin gelişiminde İç Denetçiler Enstitüsü'nün kurumsallaşmasının, üye sayısının artarak

[1] Flesher Dale L., Previts Gary John and Samson William D., "Auditing in the United States: A Historical Perspective", **Abacus,** Vol: 41, No: 1, 2005, ss. 2-14.

daha fazla dikkate alınan bir kurum olmasının, iç denetim uygulamalarına ilişkin standartlar ve ahlâk kurallarının yayınlamasının ve sertifika programları düzenlenmesinin etkileri göz ardı edilemez.

İç denetim ve iç kontrol uygulamalarına yön veren ve ana amacı finansal raporlamanın kalitesini artırmak olan bir diğer kurum da "Committee of Sponsoring Organisations of the Treadway Commission" (Treadway Komisyonu Sponsor Organizasyonlar Komitesi-COSO)'dur. COSO; Uluslararası İç Denetçiler Enstitüsü, ABD Yeminli Serbest Muhasebeciler Enstitüsü, ABD Muhasebeciler Birliği, Yönetim Muhasebecileri Enstitüsü ve Finans Yöneticileri Derneği'nin destekleriyle kurulmuş ve uluslararası alanda kabul görmüş bir örgüttür.

COSO tarafından 1992 yılında "İç Kontrol Çerçevesi" ve 2004 yılında da özet halinde "Kurumsal Risk Yönetimi Çerçevesi"nin yayınlanması iç denetim mesleğinin gelişimine ve mesleğin önündeki krizleri aşmasına yardımcı olmuştur.

Bu kısımda, tarihi sıralaması içinde iç kontrol ve kurumsal yönetime yön veren ulusal ve uluslararası çalışmalar ile raporlar ele alınarak iç denetimin çerçevesi çizilmeye çalışılacaktır.

İç kontrol sistemine ilişkin yapılan çalışmaların başında, ABD'de 1987 yılında Treadway Komisyon'u tarafından yayınlanan Treadway raporu gelmektedir. Sözkonusu raporda finansal raporlara yansıyabilecek hileli davranışların önlenmesi ve kurumsal yönetim sorunları ele alınmış ayrıca genel kabul görmüş bir iç kontrol tanımının yokluğuna dikkat çekilmiştir[2].

COSO tarafından yapılan çalışmalar sonunda 1992 yılı Eylül ayında "İç Kontrol Çerçevesi" yayınlanmıştır. Çalışmanın ileriki bölümlerinde incelenecek olan bu raporda; iç kontrol tanımı ve iç kontrol sisteminin etkinliğini değerlendirme ilkeleri yer almaktadır[3].

1992 yılında İngiltere'de COSO benzeri bir organizasyon olan Cadbury Komite'si tarafından Cadbury Rapor'u yayınlanmıştır. Raporda finansal raporlamanın kalitesinin artırılması çerçevesinde iç kontrol sistemi ve kurumsal

[2] Treadway Commission, **Report of the National Commission on Fraudulent Financial Reporting,** USA, 1987.
[3] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Internal Control - Integrated Framework,** AICPA, USA, September 1992.

yönetimin geliştirilmesi konuları incelenmiş, ayrıca iç kontrol sisteminin risklerin tanımlanmasına ilişkin süreci içermesi gerektiği vurgulanmıştır[4].

ABD ve İngiltere'nin yanısıra iç kontrol sistemi üzerine çalışmaların yapıldığı bir başka ülkede Kanada'dadır. 1995 yılında Kanada'da "Canadian Institute of Chartered of Accountants" tarafından "Guidance on Control" yayınlanmıştır. Kısaca CoCo raporu olarak da isimlendirilen çalışmada, tarihsel olarak önceki yıllarda yayınlanan raporlardan farklı olarak iç kontrol sisteminin etkinliğini ölçmeye yönelik çeşitli kriterler ele alınmıştır[5]. Raporla ilgili bir çalışmada; kurum hedeflerinin önündeki engeller ile "kontroller-riskler" ilişkilendirildiği belirlenmiştir[6].

1990'ların sonunda Cadbury raporunun yaşanan gelişmelerin gerisinde kalması ve iç kontrol sisteminin etkinlik seviyesinin açıklanması sorumluluğunun ne üst yönetim ne de iç denetçiler tarafından üstlenilmemesi, Cadbury raporunun önemli bir eksikliği olarak ön plana çıkmıştır[7]. 1999 yılında İngiltere'de "The Financial Reporting Council" tarafından "Internal Control: Guidance for Directors on the Combined Code" yayınlamıştır. Turnbull raporu olarak da isimlendirilen çalışma son olarak 2005 yılında tekrar güncelleştirilmiştir. Rapor, kurum hedeflerinin belirlenmesi, iç kontrol sisteminin risk odaklı yürütülmesi çerçevesinde risk tanımlamaları ve risk değerlemeleri, organizasyon içinde iç denetimin rolü, üst yönetim-denetim komitesi ve diğer risk birimleri arasındaki ilişkilere yoğunlaşmıştır[8].

Uluslararası alanda kabul görmüş bir diğer çalışma da Afrika'da 2002 yılında yayınlanan ve King Raporu olarak bilinen "The King Report on Corporate Governance for South Africa" isimli çalışmadır. Rapor yönetim ve yöneticiler, risk yönetimi, iç denetim, raporlama, muhasebe ve denetim başlıklarından

---

[4] Cadbury Committee, **Report of Committee on the Financial Aspects of Corporate Governance,** UK, 1992.
[5] Canadian Institute of Chartered of Accountants, **Guidance on Control,** Canadian Institute of Chartered of Accountants, Canada, 1995.
[6] Spira Laura F. and Page Michael, "Risk Management: The reinvention of internal control and the changing role of internal audit", **Accounting, Auditing & Accountability Journal,** Vol. 16, No: 4, 2003, s. 648.
[7] Page Michael and Spira Laura F., **The Turnbull Report, Internal Control and Risk Management: The Developing Role of Internal Audit**, The Institute of Chartered Accountants Scotland, UK, 2004, s. vii.
[8] The Financial Reporting Council (Turnbull Committee), **Internal Control: Guidance for Directors on the Combined Code,** UK, 1999.

oluşturulmuştur. Ayrıca raporun eklerinde risk yönetimi ve iç kontrol ele alınmıştır. Rapor temel olarak risk politikalarının oluşturulması, risk değerleme süreci ve risk yönetiminin incelenmesinden yönetim kurulunu sorumlu tutmaktadır[9].

Ulusal ve uluslararası kuruluşların çalışmaları sonucunda yayınlanan raporlar iç kontrol sisteminin benimsenmesine ve iç denetim mesleğinin gelişimine katkıda bulunmuş ayrıca iç denetimin fonksiyonlarının değişen ihtiyaçlara cevap vermesini sağlamıştır. İç denetim mesleğinin ortaya çıktığı ve büyük ölçüde meslek uygulamalarına ve yeniliklerine yön veren Amerika uygulamalarını ayrıntılı incelemek iç denetim teorilerinin anlaşılabilmesi açısından önemlidir.

1992 yılında COSO tarafından "İç Kontrol Çerçevesi"nin yayınlanması, 2000'li yılların başında yaşanan muhasebe skandallarının ardından 2002 yılı Ağustos ayında Amerika'da 'Public Accounting Reform and Investor Protection Act' (Sarbanes-Oxley) yasasının kabul edilmesi ve 2004 yılında COSO tarafından "Kurumsal Risk Yönetimi Çerçevesi"nin yayınlanması iç denetimin ulaşmış olduğu son durumu ve piyasanın değişen ihtiyaçlarına vermiş olduğu tepkileri özetlemektedir.

Enron, WorldCom ve diğer muhasebe-denetim skandalları sürecinde öne çıkan temel faktör bağımsız denetçi tarafından onaylanan finansal tablolarda karşılaşılan hatalar ve hileler olmuştur.

Bu süreçte, bağımsız denetçi tarafından sağlanan iç denetim ve danışmanlık hizmetleri (iç denetimin dış kaynaktan temini-outsource) çerçevesinde bağımsız denetçinin ne kadar bağımsız ve objektif hareket ettiği sorusu uzun süre gündemde kalmış ve bunun sonucunda Sarbanes-Oxley yasası; kurum üst yönetimi ve denetim komitesi sorumluluklarına ve bağımsız denetçi tarafından verilemeyecek danışmanlık hizmetlerine odaklanmıştır.

Yasa, bağımsız denetçi tarafından verilebilecek danışmanlık hizmetlerine sınırlama getirmenin yanısıra, Halka Açık Şirketler Muhasebe Gözetim Kurulunun (Public Company Accounting Oversight Board-PCAOB) oluşturulması ve denetim standartlarının bu kurul tarafından yayınlanması ayrıca denetim firmalarının

[9] King Committee on Corporate Governance, **King Report on Corporate Governance for South Africa,** Institute of Directors in Southern Africa, 2002.

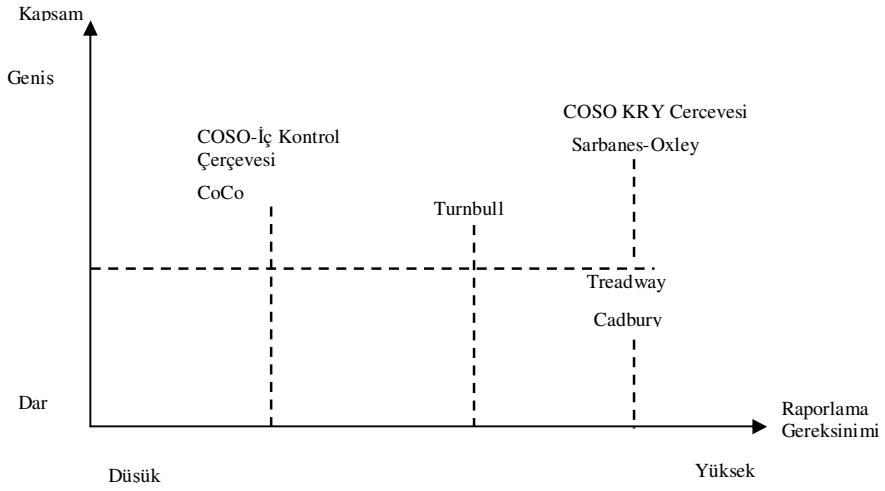
denetlenmesini söz konusu kurul faaliyetleri arasına almak da dahil, pek çok düzenlemeyi kapsamaktadır[10].

Aynı zamanda yasada, üst yönetimin ve yönetim kurulunun sadece finansal kökenli risklere değil kurum genelini ilgilendiren bütün risklere -operasyonel, sosyal ve çevresel risklerde dahil- odaklanmaları gerekliliği vurgulanarak, COSO tarafından "Kurumsal Risk Yönetimi Çerçevesi"nin yayınlanmadan önce, kurumsal risk yönetimi mantığının kabul görmesi yönündeki ilk adımlar da atılmıştır[11].

Söz konusu yasada, iç denetime ilişkin düzenlemeler iç denetim biriminin organizasyon içindeki yapısı da göz önünde bulundurularak denetim komitesi ve üst yönetim sorumluluk alanları kapsamında ele alınmıştır.

2000 yılına kadar yaşanan süreçte, iç kontrol alanında yapılan çalışmaların zamanla daha sıkı raporlama gereksinimlerinden daha gevşek raporlamaya kaydığı öte yandan kapsamın ise genişlediği dikkatleri çekmektedir[12]. Raporlama gereksinimine yönelik bu ilişkinin Sarbanes-Oxley yasası ve COSO Kurumsal Risk Yönetimi çerçevesi ile birlikte değiştiği ve raporlama gereksiniminin arttığı gözlenmektedir. Kuşkusuz bu durum muhasebe skandalları ile sonuçlanan ve raporların kurum CEO'ları tarafından imzalanmadığı diğer bir ifadeyle raporlara ilişkin sorumlulukların yöneticiler tarafından üstlenilmek istenilmemesi gerçeğiyle doğrudan ilişkilidir.

[10] USA Congress, **Sarbanes-Oxley Act of 2002**, 30 July 2002.
[11] Matyjewicz George and D'arcangelo James R., "ERM Based Auditing", **Internal Auditor,** November/December 2004, s. 8.
[12] Spira and Page, "Risk Management: The reinvention of internal control and the changing role of internal audit", s. 650.



Şekil 1: Genişleyen İç Kontrol Çerçevesi

Kaynak: Spira Laura F. and Page Michael, "Risk Management: The reinvention of internal control and the changing role of internal audit", **Accounting, Auditing & Accountability Journal,** Vol. 16, No: 4, 2003, s. 651'den alınarak geliştirilip güncelleştirilmiştir.

Yukarıda yer alan şekil iç kontrol ve iç denetim alanında yaşanan gelişimi ve bu gelişimin yönünü göstermektedir. Son olarak, Sarbanes-Oxley yasası ile beraber, yönetim kurulu ve üst düzey yöneticilerin ilgi alanına finansal risklerin yanı sıra operasyonel ve çevresel riskler de girmiştir. Bu anlamda yasa ile COSO tarafından yayınlanan KRY çerçevesi öncesinde ilgililerin dikkati bütün olarak risklere toplanmak istenmiştir[13].

COSO iç kontrol çerçevesi ile beraber faaliyet temelli riskleri dikkate alan yaklaşım Sarbanes-Oxley yasası ile beraber kapsam ve raporlama gereksinmeleri bakımından zenginleşmiş ve KRY çerçevesi ile de risk yönetimi faaliyetleri ve iç denetim biriminin olası katkıları ve veri paylaşım alanları belirginleşmiştir. Şekil, kapsam ve raporlama gereksinimlerinin genişlediğini ve artık önümüzdeki süreçte risklerin ve risk yönetiminin iç kontrol ve denetim sistemlerinin ayrılmaz bir parçası haline geleceğini özetlemektedir.

1.1.2. İç Denetim Kavramı

İç denetimin tarihi gelişimi iç denetim tanımına yapılan eklemeler ve çıkarmalar incelendiğinde daha net olarak anlaşılmaktadır. Yıllar itibariyle tanımlar incelendiğinde iç denetimin muhasebe kayıtlarının kontrolü, uygunluk

[13] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 8.

değerlendirmesi, süreçlerin incelenmesi, kontrollerin değerlendirilmesi, iç kontrol sistemi etkinliğinin raporlanması, risk yönetiminin değerlendirilmesi, risk ve kontroller hakkında güvence aşamalarından geçerek son olarak kurumsal risk yönetimi temelli çalışır hale geldiği görülmektedir[14]. İç denetimin kurumsal risk yönetimi temelli çalışması tarihsel olarak geçmişte odaklanılan alanların ihmal edildiği anlamına gelmemelidir. Günümüzde odak nokta risk yönetimi sürecine kaymıştır ve sonuç olarak geçmiş yıllardaki odak noktalar iç denetimin rutin faaliyetleri haline dönüşmüştür.

İç Denetçiler Enstitüsü tarafından yapılan başlıca iç denetim tanımları ele alınacak olursa; 1947 yılında iç denetim, "yönetime hizmet amacıyla muhasebe, finans ve diğer kurum faaliyetlerinin gözden geçirilmesinin organizasyon içinde bağımsız olarak değerlendirilmesi fonksiyonu" şeklinde ifade edilmiştir[15]. Bu tanım aynı zamanda yapılan ilk resmi iç denetim tanımıdır.

1957 yılında da 1947 yılında yapılan tanıma benzer bir tanım yapılmış fakat 1971 yılına gelindiğinde yapılan tanımda "muhasebe ve finansal faaliyetlerin gözden geçirilmesi" ifadesi kaldırılmış yerine "kurum faaliyetlerinin gözden geçirilmesi" ifadesi getirilmiş ve 1957 yılındaki tanımda yer alan "yönetime hizmet" sınırlaması korunmuştur. 1990 yılında yapılan tanımda ise bir önceki tanımda yer alan yönetime hizmet sınırlaması ifadesi "kurum-organizasyona hizmet" şeklinde genişletilmiştir[16].

2000'lerin başında yaşanan muhasebe skandalları iç denetimin kapsamına işletme risklerinin de alınması gerekliliği yanında, finansal sonuçlara ilişkin sorumluluğun yönetimde olması gerçeğini ortaya çıkarmıştır.

Son olarak 2003 yılında "iç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir" şeklinde tanımlanmıştır. Ayrıca iç denetimin amacı, "kurumun risk yönetimi, kontrol ve yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek

[14] Spencer Pickett K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** John Wiley & Sons, USA, 2004, ss 10-14.
[15] The Institute of Internal Auditors, **Statement of Responsibilities,** The Institute of Internal Auditors, USA, 1990, s. 5.
[16] **a.g.e.,** s. 5.

amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olmak" şeklinde ifade edilmiştir[17].

Bu tanımla birlikte iç denetim faaliyeti risk yönetimi ve kurumsal yönetim faaliyetlerini, bu faaliyetlerin sorumluluklarını üstlenmeksizin, görev alanına almıştır. Sarbanes-Oxley yasası ile paralel olarak iç denetim standartlarında da yer aldığı şekliyle risk yönetimi ve finansal raporlamanın sorumluluğu üst yönetime aittir.

Tanımda öne çıkan temel faktörler şu şekilde ifade edilebilir[18]:

1. Bağımsızlık ve objektiflik, iç denetimin kurum içinde oluşturulmuş olması veya kurum dışından sağlanmış olması ayrımı gözetilmeksizin, denetçiler görev alanlarına giren konularda ve alacakları kararlarda bağımsız ve objektif hareket etmelidirler.

İç denetim faaliyetlerini ve denetim görüşünü etkileyecek temel faktör iç denetim elemanlarının görev sırasında bağımsızlık ve objektifliklerini kaybetmeleridir. Bağımsızlık ve objektifliği etkileyen temel faktörler sosyal baskı, ekonomik ilgi, kişisel ilişki, iç denetim süreçlerine aşinalık, kültürel-ırksal-cinsiyet önyargıları ve kavramsal önyargı olarak sıralanabilir[19].

Bağımsızlık ve objektifliğin sağlanabilmesi ancak iç denetimin normal hiyerarşi dışında tutulması ile mümkün olabilecektir. Uygulamada iç denetim birim yöneticisinin fonksiyonel olarak denetim komitesine raporlama zorunluluğu bu sorunun çözümüne yönelik bir adımdır[20]. İç denetim birimi idari olarak da kurum CEO'su veya başkanına raporlama yapmalıdır[21].

---

[17] The Institute of Internal Auditors Research Foundation (IIARF) -Uluslararası İç Denetim Enstitüsü, **International Standards for the Professional Practice of Internal Auditing,** The Institute of Internal Auditors, USA, 2003, Çeviren Türkiye İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** İstanbul, 2003, s. v.

[18] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Sridhar Ramamoorti, **Internal Auditing: History, Evaluation, and Prospects,** Chapter 1, The Institute of Internal Auditors, USA, 2003, s. 12, Spencer Pickett K. H., **The Internal Auditing Handbook,** John Wiley & Sons, USA, 2003, s. 239., Chapman Christy and Anderson Urton, **Implementing the Professional Practices Framework,** The Institute of Internal Auditors, USA, 2002, ss. 2-5.

[19] Chapman and Anderson, **a.g.e.,** ss. 34-37.

[20] Griffiths David, **Risk Based Internal Auditing: An introduction,** http://www.internalaudit.biz, Version 2.0.3., 15 March 2006, s. 4.

[21] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 1110-2.

2. Güvence ve danışmanlık faaliyetleri de dahil edilerek iç denetimin kapsamı genişletilmiştir. Bu eklemelerle birlikte iç denetim birimi pro-aktif ve müşteri odaklı hale gelmiş ayrıca kontrol, risk yönetimi ve kurumsal yönetim sorunları hakkında yönetime danışmanlık ve güvence hizmeti vermeye başlamıştır.

Tanım iç denetim faaliyetlerinin pro-aktif olarak yürütülmesi gerekliliğine ışık tutmaktadır. Geleneksel denetim olay meydana geldikten sonra tepki verirken; kurumsal risk yönetimi temelli denetim, yaklaşımıyla birlikte olayın ortaya çıkma olasılığı üzerine iç denetim faaliyeti önlemlerini almakta ve kurumun amaçlarına ulaşmasına katkıda bulunmaktadır. Denetimin pro-aktif hareket etmesinde, KRY sisteminden aktarılacak verilerin ve KRY safhalarından risk tanımlama aşamasında ne kadar titiz çalışıldığının etkisi küçümsenemez.

3. "Kurum faaliyetlerini geliştirmek ve onlara değer katmak" ifadesi tanıma eklenerek iç denetimin kuruma yapacağı katkılarla kurumun amaçlarına ulaşmasında denetimin, etkinliğinin artırıldığı vurgulanmaktadır.

4. Geçmiş yıl tanımlarından farklı bir şekilde hem iç denetimin hizmet alanı genişletilmiş ve hem de organizasyon bir olarak bütün kurum amaçlarına ulaşılması açısından ele alınmıştır.

5. İç denetimin ufkunun genişletildiği bu tanımla birlikte kurumsal yönetim ve risk yönetimi de kapsam alanına alınmıştır.

6. İç denetim, profesyonel standartları bulunan, en iyi uygulamaların geliştirildiği ve yaygınlaştırıldığı, iç denetçinin mesleki becerilerini kaybetmeden iç denetim uygulamalarının standartlaştırıldığı, sistemli ve disiplinli bir yaklaşımdır.

Bu tanımlamaların yanısıra denetim ve risk yönetimi alanında çalışmaları ile denetim meslek uygulamalarına katkısı olan COSO'nun KRY çerçevesi isimli raporunda da İç Denetim Enstitüsü'nün tanımına benzer bir açılıma gidilmiştir. Sözkonusu raporda "iç denetim; yönetime, yönetim kuruluna ve denetim komitesine işletme kurumsal risk yönetim sistemi süreçlerinin incelenmesi, değerlendirilmesi,

raporlanması ve etkinlik ve yeterliliğinin artırılmasına yönelik önerilerin sunulması konularında destek verir" şeklinde ifade edilmiştir[22].

Genel olarak güvence, yatırımcılar ve karar alıcılar için finansal nitelikteki bilgiler ve işletme başarısının ölçümlenmesi ile ilgili olarak verilen ve bağımsız olması gereken bir hizmettir[23]. İç denetçilerin güvence ve danışmanlık hizmetlerini verirken bağımsızlık konusunda hassas davranmaları gerekmektedir. Kuşkusuz iç denetim biriminin yürüttüğü bir faaliyetin yine iç denetim tarafından denetlemesi, denetimin bağımsızlığına zarar vermesi kaçınılmazdır.

1.1.3. Risk Yönetimi Temelli İç Denetime Uzanan Süreç

Geleneksel iç denetimden risk yönetimi temelli iç denetime uzanan süreç; kuşkusuz işletmelerin değişen ihtiyaçlarından, küreselleşme sürecinin işletmeler üzerindeki etkilerinden, yaşanan teknoloji ağırlıklı değişimlerden ve bunun sonucu değişen iç ve dış ortamdan son olarak da denetim sisteminin kendini sorgulamasına ve yenilemesine-değişimine neden olan muhasebe-ekonomi temelli krizlerden etkilenmiştir.

Bunların yanısıra risk yönetiminde yaşanan gelişmeler de kaçınılmaz olarak iç denetimi etkilemiştir. Etkileşimin ana noktası risklerin yönetiminde kontrollerin önemi ve risk yönetimi sisteminin izlenmesi ve etkinlik değerlemesine olan ihtiyaçtır[24].

Bütün bu sıralanan faktörler yöneticilerin sürekli değişen ve gelişen küresel rekabet ortamında kurum faaliyetlerini etkin yürütebilmeleri için kurumsal yönetimin temel yapı taşı olan riskleri daha fazla dikkate almalarına neden olmuştur. Kurum içinde risk yönetiminin artan önemi iç denetim mesleğinde odak noktanın risklere kaymasına neden olmuştur[25].

Risk olgusu denetim yaklaşımları açısından "kontrol kökenli riskler" ve "işletme temelli riskler" olarak iki farklı şekilde ele alınacak fakat çalışma genelinde

---

[22] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** AICPA, USA, 2006, ss. 1-15.
[23] Ersin Güredin, **Denetim ve Güvence Hizmetleri,** İstanbul, Arıkan, 11. Bası, 2007, s. 4.
[24] PricewaterhouseCoopers, **Internal Audit 2012,** PricewaterhouseCoopers, USA, 2007, s. 12.
[25] McNamee David and Selim Georges, **Risk Management: Changing the Internal Auditor's Paradigm,** The Institute of Internal Auditors, USA, 1998, s. 2.

risk ifadesiyle genel olarak bütün işletme faaliyetlerini kapsayan işletme temelli riskler dikkate alınacaktır.

Denetimde yaşanan değişim, farklılaşan denetim yaklaşımlarından izlenebilir. Uluslararası İç Denetçiler Enstitüsü'nün kurulmasından sonra yaklaşık son 60 yılda kabul gören denetim yaklaşımları şu şekilde sıralanabilir:

- Kontrol temelli denetim,
- Süreç temelli denetim,
- Risk temelli denetim,
- Risk yönetimi temelli denetim.

1980'li yılların öncesinde yaygın olarak kabul gören ilk iç denetim yaklaşımı kontrol temelli denetimdir. Bağımsız denetimin bir uzantısı olarak da ifade edilebilecek olan kontrol temelli denetimde denetçi kanunlara, yönetmeliklere, politika ve prensiplere uygunluğu onaylar, bağımsız denetimin kapsamını daraltmak için gerekli test ve doğrulama işlemlerini gerçekleştirir, ayrıca anahtar kontrollerin kurum faaliyetlerini destekleyip desteklemediğini doğrular[26].

Denetim alanında kabul gören ikinci yaklaşım operasyonel denetim olarak da ifade edilen süreç temelli denetim yaklaşımıdır ve 1980'li yıllarda ön plana çıkmıştır. Süreç temelli denetim, kurum içi süreçlerin, faaliyetlerin etkinliği, etkililiği ve tasarımlarının değerlendirilmesine önem vermektedir. Bu yaklaşım, kontrol temelli denetimle karşılaştırıldığında iç denetçileri kuruma artı değer sağlama yönünde daha fazla desteklemektedir[27].

Risk temelli denetim terimi 1992 yılında COSO tarafından yayınlanan "İç Kontrol Çerçevesi" isimli raporla birlikte kullanılmaya başlanmıştır. O yıllarda yaygınlaşan risk odaklı denetim yaklaşımı, kontrol kaynaklı riskler üzerine yoğunlaşmış ve bu riskler denetim süreçlerine yansıtılmaya çalışılmıştır. Risk odaklı

[26] Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005, s. 3.03.
[27] Sobel, **a.g.e,** s. 3.04.

denetim de, kontrol riskinin dışındaki riskleri dikkate alınmamakta yani işletme temelli riskler gözardı edilmektedir[28].

Zamanla yaşanan değişim, iç denetimde odak noktanın uyumluluk risklerinden işletme kökenli risklere kaymasına neden olmuştur. Fakat bu durum uyumluluk risklerinin ihmal edildiği anlamına gelmemektedir. Bu yeni süreç risk yönetimi temelli iç denetim olarak ifade edilebilir.

Phil Griffiths tarafından İngiltere Borsası (Financial Times Stock Exchange) FTSE 250 endeksinde yer alan şirketler üzerinde karşılaştırmalı olarak 2000, 2002 ve 2004 yılları dikkate alınarak yapılan araştırmanın sonuçları yaklaşık son 15 yıl içinde yaşanan değişimi net olarak özetlemektedir[29].

Tablo 1: Fonksiyonlar Arası Öncelik - Odak Noktası

	2000 Yılı Oranları (%)	2002 Yılı Oranları (%)	2004 Yılı Oranları (%)
İşletme Kökenli Risklere Yönelik	40	72	89
Finansal Sistem Odaklı	23	7	1
Operasyonel Sistem Odaklı	20	10	2
Uygunluk Odaklı	10	6	1
İç Danışmanlık	4	1	1
Para Değerli	2	2	0
Kurumsal Yönetim	1	2	6

Kaynak: Griffiths Phil, **Risk-Based Auditing,** Gower Publishing, USA, 2005, s. 7.

Sözkonusu araştırmanın 2000 yılı sonuçlarına göre iç denetimin tüm faaliyetler arasında işletme kökenli risklere % 40 oranında zaman ve kaynak ayırdığı görülmekteyken aynı araştırmanın 2004 yılı sonuçlarına göre ise bu oran % 89'a çıkmıştır. Buna paralel olarak finansal ve operasyonel sistem odaklı denetim faaliyetleri, uygunluk odaklı faaliyetler ve diğer faaliyetlerin ağırlığı zamanla azalmıştır[30]. Ağırlıkları azalan faaliyetler rutin iç denetim faaliyetleri arasında yerini almaktadır. Bu durum, bu faaliyetlerin tamamıyla terk edildiği anlamına gelmemektedir.

Risk yönetimi temelli denetim, işletme hedeflerinin geniş çerçevede ele alındığı, risk yönetimi kapasitesinin genişlediği ve risk yatıştırma-tutumu

[28] Galloway David, **Internal Auditing: A Guide for the New Auditor,** The Institute of Internal Auditors, USA, 1995, ss. 36-37.
[29] Griffiths Phil, **Risk-Based Auditing,** Gower Publishing, USA, 2005, s. 7.
[30] Griffiths Phil, **a.g.e.,** s. 8.

tekniklerinin zenginleştirildiği risk odaklı denetimin kapsam ve araçlarının gelişmiş halidir.

Tablo 2: Denetim Yaklaşımlarının Karşılaştırılması

	Kontrol Temelli Denetim	**Süreç Temelli Denetim**	**Risk Temelli Denetim**	**Risk Yönetimi Temelli Denetim**
Hedef	Yönetmeliklere ve mevzuata uygunluk	Süreç etkinliği ve etkiliği	Kontroller ve süreçlerin risklerin yatıştırılması karşısında etkililikleri	Kurum hedeflerine ulaşma ve risklerin yatıştırılması-optimizasyonunda risk yönetimi faaliyetlerinin etkililiği
Yaklaşım	Uygunluk için denetim ve kılavuzların anlaşılması	Mevcut süreçlerin ve en iyi uygulamaların karşılaştırılması	Anahtar iş risklerinin tanımlanması ve risklerin yatıştırılmasına yönelik kontrollerin değerlendirilmesi	Hedeflerin anlaşılması, ilgili risklerin tanım-lanması, tolerans seviyelerinin anlaşılması, performans ve risk ölçümlerinin tanımlanması ve risk yönetimi etkinliğinin değerlendirilmesi
Odak	Uygunluk istisnalarının ve hatalarının belirlenmesi	Mevcut süreçler ve en iyi uygulamalar arasındaki boşlukların belirlenmesi	Anahtar risklerinin yatıştırılmasında gerekli etkinliği göstermeyen süreçlerin ve kontrollerin belirlenmesi	Mevcut ve istenen risk yönetimi etkinliği arasındaki boşlukların belirlenmesi
Test Yaklaşımı	Uygunluk testleri ile birlikte istatistik temelli anlamlılık ve kestirimci testler	Mevcut ve en iyi uygulamaları değerlendirmeye yönelik danışmanlık yaklaşımı ve bazı uygunluk testleri	Anahtar risklere odaklanmış anlamlılık ve uygunluk testlerinin bileşimi	Anahtar hedefler ve ilgili risklere odaklanmış anlamlılık ve uygunluk testlerinin bileşimi
Tavsiyeler	Kılavuzla ilgili istisnalar veya hatalar hakkında	Özel faaliyet amaçları ile ilgili boşluklar hakkında	Anahtar risklerle ilgili istisnalar veya hatalar hakkında	Temel iş hedefleri ve risklerle ilişkili risk yönetimi etkinliği boşlukları hakkında

Kaynak: Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005, s. 3.11.

Yukarıda yer alan tabloda kontrol, süreç, risk ve risk yönetimi temelli denetim yaklaşımları denetim hedefi, yaklaşımı, denetimde odak nokta, test yaklaşımları ve denetim tavsiyeleri açısından karşılaştırmalı olarak topluca ele alınmıştır.

Farklılaşan ihtiyaçlar denetim hedeflerinin değişmesine yol açmaktadır. Kontrol temelli denetim iç kontrol faaliyetlerinin onaylanması ve etkinliğinin yükseltilmesine odaklanmıştır. İç denetçi, denetim faaliyetinin gerçekleştirilmesi sırasında "polis" gibi hareket etmekte, denetime konu faaliyetlerin yasa ve yönetmeliklere uygunluğunu araştırmaktadır.

Yaşanan değişimle birlikte risk yönetimi temelli denetim ise kurum hedeflerine ulaşma ve risklerin yatıştırılması-optimizasyonu sürecinde risk yönetimi faaliyetlerinin etkinliğini değerlendirmektedir. Bu yaklaşımda iç denetçi kurumdaki rolü itibariyle danışman pozisyonuna yakındır. Sarbanes-Oxley yasası sonrasında yaşanan süreçte iç denetçinin bağımsız ve objektif davranması gerekliliklerinin artması, iç denetim birimini organizasyonel anlamda olmasa da mantık olarak "kuruma dışarıdan bakma-yaklaşma" noktasına getirmiştir.

Kontrol temelli denetim, kurum muhasebe sisteminin anlaşılmasına ve işlemlerin detaylarına odaklanır. Denetçi finansal tabloların bütün bileşenlerini inceleyerek gerçekleştirilen işlemlerin tam ve doğru olarak kaydedildiğine ilişkin güvence sağlar. Bu nedenle uygunluk için denetim ve kılavuzların anlaşılması önemlidir[31]. Öte yandan risk yönetimi temelli denetim ise kurum iş modelinin ve süreçlerinin anlaşılması, ilgili risklerin tanımlanması, tolerans seviyelerinin anlaşılması, performans ve risk ölçümlerinin tanımlanması ve risk yönetimi etkinliğinin değerlendirilmesine yoğunlaşmaktadır[32]. Buradan sağlanan bilgi finansal tabloları etkileyebilecek riskli alanların tanımlanmasında ve denetim kaynaklarının söz konusu alanlara aktarılmasında ve dolayısıyla işletmenin amaçlarına ulaşmasını engelleyecek faaliyetlerin ortadan kaldırılmasında veya etkilerinin azaltılmasında kullanılır[33].

[31] Davies Mark, **Auditing in the New Millennium,** KPMG's Monograph 2001, 2001, s. 1.
[32] Sobel, **a.g.e,** s. 3.07.
[33] Davies, **a.g.e.,** s. 1.

Odak noktası açısından, kontrol temelli denetimde; denetçi ağırlıklı olarak zamanını planlama, teknik ve iç kontrolle ilgili ayrıntılarla temelde uygunluk faaliyetleri ile geçirirken, risk yönetimi temelli ise iç denetimde denetçi; risklerin çeşitlendirilmesi, risklerden sakınılması, risklerin paylaşılması ve risklerin transfer edilmesi konularındaki sorulara cevap arar[34]. Risk yönetimi temelli denetimle birlikte iç denetçinin kuruma değer katma fonksiyonu, kontrol temelli denetime kıyasla daha çok ön plana çıkmıştır[35].

Risk yönetimi temelli denetim, denetimin yönünü geçmişten günümüze ve geleceğe çevirmekte, bir başka ifadeyle denetimin çalışma alanını değiştirmektedir. İç denetçinin geçmişte meydana gelmiş işlere yoğunlaşması, standart hale gelmiş bağımsız değerlendirme fonksiyonlarını uygulaması, yeni bilgiler üretmesini kısıtlarken, denetimin günümüze ve geleceğe ait işlere odaklanması, risk yönetiminde aktif hale gelmesi, denetçinin organizasyonun başarısını engellemesi muhtemel ayrıntılara yönelmesinin önünü açmaktadır[36].

Kontrol temelli iç denetim iç kontrole odaklandığı için, denetçi iç kontrolün etkinliğine ve genel olarak da mevzuata uyum sürecinde ilişkin tavsiyelerde bulunur. Risk yönetimi temelli denetimde ise iç denetçi; risklerin çeşitlendirilmesi, risklerden sakınılması, risklerin paylaşılması ve risklerin transfer edilmesi konularına odaklanır[37]. Bu doğrultuda iç denetçi; kurum hedefleri ve risklere yönelik risk yönetiminin etkinliğini artırılmasına ilişkin tavsiyelerde bulunur[38]. İç denetimde odak noktanın değişimi kontrollerin ihmal edildiği anlamına gelmemelidir. Risk yönetimi temelli denetimle birlikte kontroller, ortaya çıkarıcı kontrol mekanizmalarından önleyici kontrol mekanizmalarına kaymıştır.

Risk yönetimi temelli iç denetim, kurum hedefleri, riskler karşısında yönetim toleransları, anahtar risk ölçüm yöntemleri ve risk yönetimi yetenekleri açısından risk odaklı iç denetimin geliştirilmiş halidir. Bu temel ayrıma ek olarak risk odaklı denetim, geleneksel risk yönetimine dayanması nedeniyle riskler karşısındaki tutumu

---

[34] Kishalı Yunus ve Pehlivanlı Davut, "Risk Odaklı İç Denetim ve İMKB Uygulaması", **Muhasebe ve Finansman Dergisi,** Nisan 2006, s. 82.
[35] KPMG, **The Financial Statement Audit: Why a New Age Requires an Evolving Methodologies of Large Accounting Firms,** KPMG LLP., USA, 1999, s. 9.
[36] Mcnamee David and Selim Georges, "Changing Paradigm", **Mc² Management Consulting,** http://www.mc2consulting.com/riskart8.htm, (17.11.2006).
[37] Kishalı ve Pehlivanlı, ss. 82-83.
[38] Sobel, **a.g.e,** s. 3.09.

riskleri kabul edilebilir bir seviyeye indirmeye çalışır. Diğer yandan kurumsal risk yönetimi temelli iç denetim ise riskleri kurum hedeflerine ulaşılabilecek seviyede optimize etmeye çalışmaktadır[39].

Denetimde farklılaşan odak noktası ve denetim yaklaşımlarına rağmen uygulamada dört denetim yaklaşımının da birlikte fakat kurumların, sektörlerin ve doğal olarak ülkelerin farklılaşan ihtiyaçları doğrultusunda farklı ağırlıklarda kullanıldığı gözlemlenmektedir. Örneğin bankacılık sektörü iç denetim felsefesi, daha çok kurumsal risk yönetimi temelli denetime dayanmaktayken reel sektör henüz kontrol ve risk odaklı çalışmaktadır.

1.2. KURUMSAL YÖNETİM BAĞLAMINDA İÇ DENETİM

Kurumsal yönetim kavramının ortaya çıkmasının hem yönetim temelli hem de finans temelli gerekçeleri bulunmaktadır. Ulusal ekonomilerin gelişmesi, uluslararası ekonomik ilişkilerin ve buna paralel olarak uluslararası sermaye akışkanlığının artması, şirket hissedarlarının işletme yönetimindeki etkinliklerinin azalması, şirket yönetim kurulları ve özellikle kurul içinde murahhas yönetici (CEO-Genel Müdür) unvanını taşıyan yöneticilerin verdikleri kararların öneminin artması gibi faktörler kurumsal yönetim kavramının doğuşunda etkili olmuştur[40].

Kurumsal yönetime ihtiyaç duyulmasının nedeni, hukuki alt yapı ne kadar gelişmiş ve düzenleme süreci ne kadar esnek ve gelişmelere ne kadar duyarlı olursa olsun, zaman içerisinde mevzuat ile uygulamalar arasında kaçınılmaz olarak bir boşluk oluşmasıdır. Bu boşluk yeni yasal düzenlemelerle giderilmeye çalışılmakta, ancak bu da zaman almaktadır. Kurumsal yönetim düzenlemelerinin bu boşluğun ortadan kaldırılması sürecinde önemli işlevleri bulunmaktadır[41].

Temel amacı kurumun, kurumla ilgili tüm hak sahiplerinin çıkarlarının adil bir şekilde gözetilmesi olan kurumsal yönetim, şirket ile hak sahiplerinin ve diğer menfaat sahiplerinin birbiriyle olan ilişkilerini düzenleyen ve hak sahiplerinin

---

[39] Sobel, **a.g.e,** s. 3.06.
[40] Baraz Barış, "Yönetim Kurullarının Kurumsal Yönetişim Açısından Kritik Önemi: Eskişehir'de Bir Araştırma", **3.Ulusal Bilgi, Yönetim ve Ekonomi Kongresi,** Osmangazi Üniversitesi, Eskişehir, 2004, s. 764.
[41] Doğu, **"Kurumsal Yönetim Düzenlemeleri",** Sermaye Piyasası Kurulu Meslek Personeli Derneği Dergisi, Sayı 8, Temmuz-Ağustos 2003, s. 2.

şirketten elde edeceği menfaatlerin en üst düzeye ulaştırılmasını sağlayan ilkeler bütünüdür[42].

Kurumsal yönetimin ifade edilen amaca ulaşabilmesi ancak kurumun finansal durumuna ilişkin bilgileri tam ve doğru bir şekilde ve zamanında açıklanması ile mümkün olmaktadır[43]. Bunun da gerçekleştirilebilmesi kurum içi; denetim komitesi ve iç denetim biriminin, kurum dışı ise; bağımsız denetim fonksiyonlarının etkin çalışması ile mümkündür[44].

Denetim, kurumsal yönetimin en kritik yönünü temsil etmektedir[45]. Denetim ve kurumsal yönetim hakkında yapılan çalışmalardan çıkan sonuçlar; iyi işleyen bir kurumsal yönetim sisteminin denetim risklerini azaltacağı ve denetçilerin kurumda varolan kurumsal yönetim mekanizmasının kalitesini değerlendirmek yoluyla kendi çalışmalarını buna göre ayarlayabileceği yönündedir[46]. Bunlara ek olarak, kurumsal yönetimin finansal raporlama sürecinin kalitesinin artmasına katkısı da ihmal edilmemelidir[47].

Etkin kurumsal yönetimin üzerinde inşa edilebileceği zeminin köşe taşları üst yönetim, yönetim kurulu, iç denetçiler ve dış denetçilerdir. İç denetim faaliyeti, iyi bir kurumsal yönetimin desteklenmesinde önemli bir rol oynar. Risk yönetimi, kontrol ve yönetim süreçlerinin etkinliğini değerlendirerek ve geliştirerek kurum faaliyetlerinin iyileştirilmesinde yardımcı olabilecek özel bir konuma sahiptir[48].

Bağımsız denetim açısından kurumsal yönetim mekanizması, bağımsız denetçiye, kabul edeceği müşteriye ilişkin riskleri değerlendirme, daha etkili ve yeterli denetim planı hazırlama aşamalarında yardımcı olur. Ayrıca güçlü bir

---

[42] Özeke Hergüner Bilgen, **Kurumsal Yönetim İlkeleri Uyum Raporu,** www.herguner.av.tr, 23.12.2005.
[43] Koçel, **a.g.e.,** s. 466.
[44] Archambeault Deborah S., **The Relation Between Corporate Governance Strength And Fraudulent Financial Reporting: Evidence From Sec Enforcement Cases,** University at Albany-SUNY, Working Papers, November 2002, s. 247.
[45] **a.g.e.,** s. 5.
[46] Baker C. Richard and Owsen Dwight M., "Increasing The Role of Auditing in Corporate Governance", **Critical Perspectives on Accounting,** Vol. 13, 2002, s. 785.
[47] Cohen Jeffrey, Krishnamoorthy Ganesh and Wright Arnold M, "Corporate governance and the audit process", **Contemporary Accounting Research,** Vol. 19, No 4, Winter 2002, s. 588.
[48] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2120.A1-4:1.

kurumsal yönetimin bulunduğu şirketlerin denetiminde denetçi daha az örnek büyüklüğü ile çalışır ve böylelikle test maliyetleri azaltılır[49].

Kurumsal yönetimde zayıflık ve aksaklıkların bulunması denetimin etkinliğini azaltacaktır. Bunun sonucunda yolsuzluklar, hisse değerinin düşmesi ve dolayısıyla müşteri kaybı gibi birçok olumsuzluk meydana gelir[50].

Kurumsal yönetimin sözü edilen faydaları sağlayabilmesi sistemin etkin işlerliği ile ilgilidir. Bu bağlamda iç denetim yönetmeliği ve raporu ile bağımsız denetim raporu, kurum dışı ilgililerin tarafsız ve doğru bilgi alabilmeleri için temel araçlardır.

1.2.1. İç Denetim Yönetmeliği

İç denetim yönetmeliği, iç denetim standartları çerçevesinde denetimin amaç, yetki ve sorumlulukların tanımlandığı ve denetim komitesi ile yönetim kurulu tarafından onaylanması gereken bir yönetmeliktir[51].

Söz konusu yönetmelik, iç denetim faaliyetlerinin kurum içindeki konumuna ilişkin düzenlemeleri yapmalı, iç denetim görevlerinin yerine getirilebilmesi için gerekli kayıtlara, personele, demirbaşa ve ilgili alanlara erişim yetkisini düzenlemeli ayrıca iç denetim faaliyetlerinin kapsamını tanımlamalıdır[52]. Bu özellikleriyle yönetmelik, iç denetimin vereceği danışmanlık ve güvence fonksiyonları arasındaki dengeyi ve kurum organizasyon yapısında iç denetim ve kurumsal yönetim, risk yönetimi ve kontrol sistemleri arasındaki ilişkiyi belirlemektedir[53].

Yönetmelik aynı zamanda, denetim komitesi ve iç denetim birimi arasındaki ilişkiyi tanımlamalıdır. Bu durum, üst yönetime iç denetim biriminin uygulamada sorunlarla karşılaşması halinde kurum üst kuruluna, denetim komitesine, ulaşabileceği mesajını içermektedir[54]. Pratikte bu mesajın işlerlik kazanabilmesi de

---

[49] Cohen ve diğerleri, ss. 577-584.
[50] Active Academy Ar-Me, "Sürdürülebilir Kurumsal Yönetimin Şartı Etkinlik", **Activeline,** Aralık 2003, s. 2.
[51] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 1000-1.
[52] The Institute of Internal Auditors, Glossary of Terms, http://www.theiia.org, 10.09.2006.
[53] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 51.
[54] Moeller Robert R., **Brink's Modern Internal Auditing,** John Wiley & Sons, 2005, s. 182.

denetim komitesi üyelerinin bağımsızlık dereceleri ve uzmanlık seviyeleri ile ilgilidir.

İç denetim yönetmeliği kurumların ihtiyaçlarına göre farklılık gösterebilse de genellikle yönetmelikte yer alan ana başlıklar aşağıdaki gibidir[55]:

- Hedefler – iç denetim biriminin hedefleri.
- Misyon – kurum misyonu çerçevesinde iç denetim biriminin misyonu.
- Raporlama – raporlama yapma zorunluluğu olan birimler ve diğer üçüncü şahıslara yapılacak raporlamanın sınırları.
- Sorumluluklar – iç denetim faaliyetinin sorumlu olduğu alanlar.
- Yetkiler – denetim faaliyetlerinin gerçekleştirilmesi esnasında iç denetim çalışanlarının ve birim yöneticisinin yetkileri.
- Standartlar – faaliyetlerin gerçekleştirilmesi sırasında uyulacak standartlar ayrıca varsa yönetmelik ve diğer yasal düzenlemelerin açıklanması.

Bunlara ek olarak iç denetim yönetmeliği kısa ve anlaşılır olmalı, iç denetim biriminin bağımsızlık olgusu vurgulanmalı ayrıca gerekiyorsa "denetim ahlak kuralları" yönetmeliğe eklenmelidir. İç denetim yönetmeliği hakkında ifade edilenler yönetmeliğin çerçevesini çizmektedir. Bunların varlığı yönetmeliğin sorunsuz işleyeceği anlamına gelmemektedir. Eğer yönetmelik üst yönetim tarafından desteklenmiyorsa uygulamada pek çok sorunla karşılaşılabileceği de unutulmamalıdır[56].

Kurumsal risk yönetimi politikaları çerçevesinde ve denetim komitesinin de ihtiyaçları dikkate alınarak hazırlanan iç denetim yönetmeliği, hızlı değişen çevre koşullarında ve denetimin farklılaşan görevlerine uygun olarak denetim komitesi tarafından güncellenmelidir[57]. Fakat uygulamada çoğunlukla iç denetim yöneticisi tarafından güncellendiği dikkatleri çekmektedir[58].

---

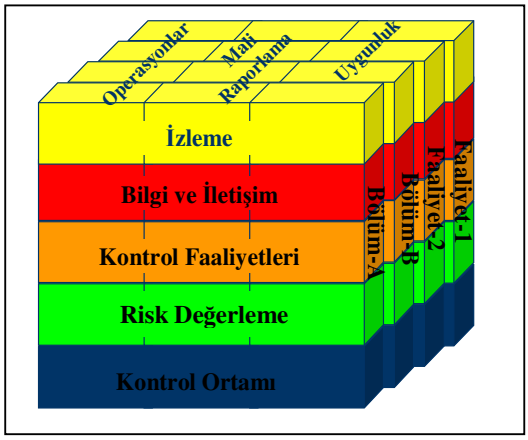
[55] FTI Consulting Inc., **Internal Audit Charter,** 28.04.2004., The Bellsouth Corporation, **Internal Audit Charter,** 2005., Bank For International Settlements, **Internal Audit Charter,** 20.03.2003.
[56] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 251.
[57] Spencer Pickett K. H., **Auditing The Risk Management Process,** John Wiley & Sons, USA, 2005, s. 39.
[58] Moeller, **Brink's Modern Internal Auditing,** s. 182.

1.2.2. İç Denetim - İç Kontrol Sistemi İlişkisi

1992 yılında COSO tarafından yayınlanan "İç Kontrol Çerçevesi", iç kontrol tanımına, kurumların iç kontrol sistemlerinin değerlendirilmesine ve geliştirilmesine ilişkin bir çerçeve sunar.

COSO iç kontrol çerçevesinde iç kontrol "bir kurumun yönetim kurulu, üst yönetimi ve çalışanlarından etkilenen ve operasyonların etkinliği ve verimliliğine, finansal raporlamanın güvenilirliğine ve yürürlükteki kanun ve düzenlemelere uyuma ilişkin makul düzeyde güvence sağlayan bir süreç[59]" şeklinde tanımlanmıştır. Genel olarak değerlendirilecek olursa iç kontroller kurumun hedeflerine ulaşma olasılığını artıran yönetim faaliyetleridir.

İç kontrol tanımında yer alan hedeflere ulaşılabilmesi birbiri ile ilişkili beş bileşenin varlığına bağlıdır. İç kontrol sisteminin bileşenleri; kontrol ortamı, risk değerleme, kontrol faaliyetleri, bilgi ve iletişim ile izlemedir.



Şekil 2: COSO İç Kontrol Küpü

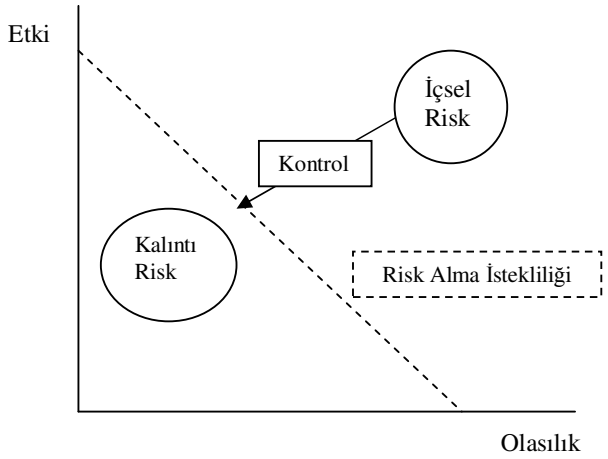
Kaynak: Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Internal Control – Integrated Framework,** USA, 1992, s. 12.

Tanımda da yer aldığı şekliyle iç kontrol sisteminin amaçları küpün dikey katmanında operasyonlar, mali raporlama ve uygunluk olarak yer almıştır. Küpün yatay katmanı, kontrol ortamı, risk değerleme, kontrol faaliyetleri, bilgi ve iletişim ile izleme'den meydana gelmektedir. Küpün üçüncü boyutu ise bölümler ve faaliyetler şeklinde ayrımlandırılmıştır.

[59] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **"Internal Control-Integrated Framework",** s. 5.

Risk yönetimi ile ilişkisi bakımından, iç kontrol sistemi risk yönetim sisteminin temeli olarak kabul edilebilir. İç kontrol sistemi, yönetime işletme faaliyetlerinin doğasında var olan risklere karşı, bu risklerin kontrolü ve yönetimi konusunda destek vermektedir[60]. Bu destek-yardım aslında risk yönetiminin ilk adımını oluşturmaktadır. Eğer kurum hedeflerine ulaşmayı engelleyecek herhangi bir risk söz konusu değilse kontrol önlemlerine de gerek olmayacaktır[61].

Şekil 3'te risk yönetimi içinde kontrollerin yeri; risklerin kurum risk alma istekliliği sınırları içine indirgenmesi kabulü çerçevesinde ele alınmaktadır.



Şekil 3: Risk Yönetimi İçinde Kontrollerin Yeri

Kaynak: Griffiths David, **Risk Based Internal Auditing: Three views on implementation,** www.internalaudit.biz, Version 1.0.0., 30 January 2006, s. 5.

Risk alma istekliliği çerçevesinde tasarlanan kontroller, risklerin bir kısmının ortadan kaldırılmasını (içsel risk) sağlarken, alınan kontrol önlemlerine rağmen kaldırılamayan riskler kalıntı riskler şeklinde ifade edilir. İç denetçi kontrollerin etkin bir şekilde çalıştığına ilişkin güvence verir ve kontrollerin iyileştirilmelerine ilişkin önerilerde bulunur[62]. Bu açıdan iç denetim faaliyeti, temelde kurum iç kontrol sisteminin etkinliğini değerlemek amacıyla gerçekleştirilmektedir.

1.3. DENETİM AÇISINDAN RİSKLER VE YÖNETİMİ

Denetim faaliyeti özünde güvence ve danışmanlık hizmetlerinin bir bileşimidir. İç denetim biriminin, güvence ve danışmanlık hizmeti verebileceği

[60] Galloway, **a.g.e.,** s. 35.
[61] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 3.
[62] Griffiths David, **Risk Based Internal Auditing: Three views on implementation,** http://www.internalaudit.biz, Version 1.0.0., 30 January 2006, s. 5.

alanlar sorumluluk ve bağımsızlık kısıtları nedeniyle tartışmalı bir alandır. İç Denetçiler Enstitüsü (Birleşik Krallık-İrlanda) tarafından yayınlanan rapor bu alandaki boşluğu doldurmuştur.

1.3.1. Denetim Açısından Riskler ve Kontroller

Farklı bilim dallarında pek çok risk tanımı ile karşılaşmak mümkün olmakla birlikte risk genel olarak organizasyonun hedeflerine ulaşmasını engelleyen her türlü olay olarak ifade edilebilir[63]. Risk işletmenin uyguladığı stratejilerden kaynaklanmaktadır, stratejinin yokluğu halinde ise riskten söz edilemeyecektir[64].

Risk temelde iki bileşenden oluşmaktadır; belirsizlik ve etki. Bununla beraber "risk = belirsizlik" genellemesi yanlıştır. Çünkü belirsizlik bir etkiye neden olmayabilirken riskin en önemli sonucu etkidir. Ayrıca belirsizlik durumunda meydana gelecek olayın olasılığı bilinmezken, risk sözkonusu olduğunda olasılıklar bilinmektedir[65].

İster özel sektör işletmesi ister kamu veya sivil toplum kurumu olsun bir amacı olan ve bu amaca yönelik faaliyetlerde bulunan her kurum belirli bir risk ortamında faaliyetlerini sürdürür. Risklerin tamamıyla ortadan kaldırılması ne mümkündür ne de optimumdur. Ancak riskler kabul edilebilir sınırlar içinde tutulabilirler. Kurumsal Risk Yönetimi aşamaları içinde açıklanacağı şekliyle kabul edilebilir risk sınırı da, başta kurum risk kültürü olmak üzere kurumun risk alma istekliliği ve başkaca diğer faktörlerden de etkilenir. Geleceğin belirsizliğinden kaynaklanan riskleri azaltmanın, kabul edilebilir sınırlar içinde tutmanın en temel yolu da kontroller oluşturmaktır[66].

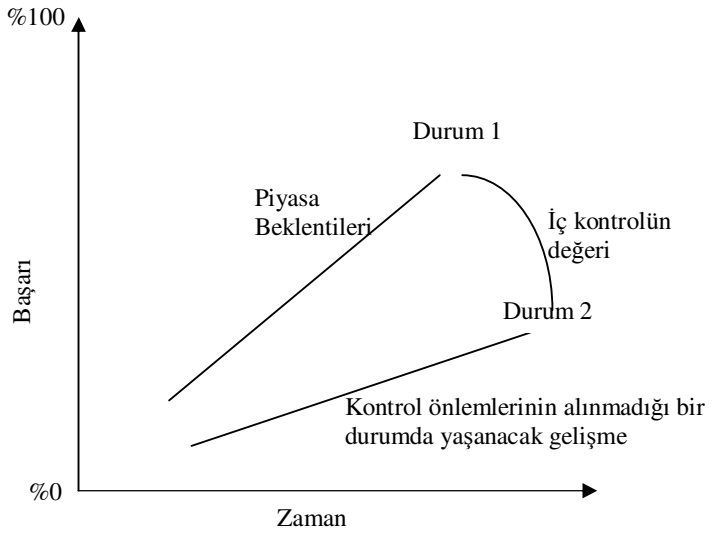
Tarihsel olarak incelendiğinde muhasebe ve iç denetim aşamalarının faaliyet planlarının uygulama sonuçlarının değerlendirilmesini ve ölçümünü içerdiği fakat riskleri içermediği görülmektedir[67]. 1992 yılında COSO İç Kontrol küpünün

---

[63] The Institute of Internal Auditors, **Glossary of Terms.**
[64] Sobel, **a.g.e,** s. 1.03.
[65] Hillson David and Murray-Webster Ruth, **Understanding and Managing Risk Attitude,** Gower Publishing, USA, 2005, s. 5.
[66] Lam James, **Enterprise Risk Management From Incentives to Control,** John Wiley & Sons, USA, 2003, s. 38.
[67] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Kinney William R., **Auditing Risk Assessment and Risk Management Processes,** Chapter 5, s. 133.

yayınlanmasıyla birlikte denetçi ve muhasebeciler iç kontrol ve riskleri muhasebe hatalarından farklı algılamaya başlamışlardır[68].

90'lı yıllar boyunca tartışma konusu olan "iç kontrol risk yönetiminin bir parçası mıdır? yoksa risk yönetimi kontrolün bir elemanı mıdır?" sorusu; COSO iç kontrol çerçevesinde risk değerlemesinin iç kontrol sisteminin bileşenleri arasında gösterilmesi ve COCO raporunda "kontroller risk tanımlamaları ve yatıştırma faaliyetlerini içermelidir" ifadesinin yer almasıyla cevap bulmuştur[69].



Şekil 4: Kontrollerin Risk Yönetimine Katkısı

Kaynak: Pickett Spencer K. H. and Pickett Jennifer M., **Auditing For Managers The Ultimate Risk Management Tool,** John Wiley & Sons, USA, 2005, s. 75.

Kontroller temel olarak risklerin kabul edilebilir seviyeye çekilmesine katkıda bulunurken, genel olarak değerlendirildiğinde kurumun faaliyetlerinin istenen amaca ulaşmasına katkıda bulunur. Kurum tarafından verilen bir hizmete ilişkin örnek şekilde gösterilmiştir. Şekil 4'te, Durum 2 kontrol önlemleri alınmadığında kurumun ulaşabileceği başarı derecesini göstermektedir. Durum 1 ise kontrol önlemlerinin alındığı ve piyasa beklentilerine uygun faaliyetin gerçekleştirilmesini gösterir.

[68] Knechel Robert W., "The Business Risk Audit: Origins and Obstacles (and Opportunities?)", **3rd EARNet Symposium,** Amsterdam, September 2005, s. 12.
[69] Page Michael and Spira Laura F., **The Turnbull Report, Internal Control and Risk Management: The Developing Role of Internal Audit,** s. 15.

Durum 1 ve 2 arasındaki başarı karşılaştırması kontrollerin katkısını ortaya koymaktadır[70].

1.3.2. Bütünleştirilmiş Risk Yönetimi ve İç Denetim

Günümüzde iç kontrol, iç denetim ve risk yönetimi sistemi, sadece finansal raporlama ve mevzuata yönelik uyumluluk risklerini değil aynı zamanda işletmelerin günlük faaliyetlerinin olağan bir şekilde yürütülmesinin ve işletmelerin orta ve uzun vade hedeflerine ulaşmasının önünde yer alan riskler de dahil olmak üzere kurumun genelini ilgilendiren riskleri uzun vadeli bir bakış açısıyla ele almak zorundadır.

İç denetim tanımında da yer aldığı şekliyle iç denetim faaliyeti, sistematik ve disiplinli bir yaklaşımla, risk yönetimi ve kontrolleri değerlendirmeli bu sistemlerin iyileştirilmesine katkıda bulunmalıdır.

İç denetim biriminin risk yönetimi sürecinde dört farklı rolü olabilir. İşletmede kurumsal risk yönetimi mevcutsa; iç denetim biriminin kurum risk yönetimi sürecinde hiç rolü olmayabilir veya iç denetim planının bir parçası olarak risk yönetim sürecini denetleyebilir. Diğer taraftan işletmede kurumsal risk yönetimi sistemi yoksa iç denetim birimi risk yönetimi sürecine faal ve kesintisiz bir destek sağlayabilir veya risk yönetimi sürecini üstlenebilir[71]. İç denetim biriminin bu süreçte üstleneceği rol üst yönetim ve denetim komitesi tarafından iç denetim yönetmeliği aracılığıyla belirlenir[72].

İç denetim biriminin kurumsal risk yönetimi konusunda üstlenmemesi gereken görevler hakkında literatürde bir görüş birliği bulunmakla beraber, iç denetimin üstlenmesi gereken görevler hakkında bir uzlaşma yoktur. Bazı araştırmacılar, iç denetim biriminin sadece kurumsal risk yönetiminin son aşaması olan "izleme" fonksiyonunu yerine getirmesi gerektiğini savunurken bazı araştırmacılar ise "kurumsal risk yönetiminin bütün aşamalarında iç denetim birimi aktif olmalıdır" görüşünü savunmaktadırlar[73].

---

[70] Pickett Spencer K. H. and Pickett Jennifer M., **Auditing For Managers The Ultimate Risk Management Tool,** John Wiley & Sons, USA, 2005, s. 75.
[71] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2100-3. ve 6.
[72] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 173.
[73] Beasley Mark S., Clune Richard and Hermanson Dana R., "Enterprise Risk Management and the Internal Audit Function", **Coles College of Business Kennesaw State University Working Papers,** December 2004, s. 6.

Bu tartışmalar üzerine İç Denetçiler Enstitüsü (Birleşik Krallık-İrlanda) yayınladığı gözden geçirme raporu ile soruna açıklık getirmiştir. Raporda, iç denetim biriminin, KRY çerçevesinde yürüttüğü fonksiyonların ötesinde denetimin bağımsızlığına ve objektifliğine zarar vermeyecek şekilde görevler üstlenmesi gerektiği vurgulanmaktadır. Bunlar; iç denetim birimi tarafından üstlenilebilecek temel görevler, iç denetimin şartlı olarak üstlenebileceği görevler ve iç denetimin üstlenmemesi gereken görevler olarak üç başlık altında ele alınmıştır[74].

1. Kurumsal Risk Yönetimi Kapsamındaki Temel İç Denetim Görevleri
    a. Risk yönetimi süreçleri hakkında güvence verme,
    b. Risklerin doğru bir şekilde değerlendirildiğine ilişkin güvence verme,
    c. Risk yönetimi süreçlerini değerlendirme,
    d. Önemli risklerin raporlamasını değerlendirme,
    e. Önemli risklerin yönetilmesini gözden geçirme,
2. Şartlı Olarak Üstlenilebilecek İç Denetim Görevleri
    a. Risklerin tanımlanmasına ve değerlendirilmesine yardım etme (Görüşme, çalıştay gibi),
    b. Risk tutumları konusunda yönetimi eğitme,
    c. KRY faaliyetlerini koordine etme,
    d. Risklerin raporlamasını konsolide etme,
    e. KRY çerçevesini yürütme ve geliştirme,
    f. KRY'nin oluşturulmasına öncülük etme,
    g. Yönetim kurulunun onayına sunulacak risk yönetimi stratejisini geliştirme,
3. İç Denetimin Üstlenmemesi Gereken Görevler
    a. Risk alma istekliliği sınırlarının belirlenmesi,
    b. Risk yönetimi süreçlerinin kuruma empoze edilmesi,
    c. Riskler hakkında yönetim adına güvence verilmesi,
    d. Risk tutumu kararının alınması,
    e. Yönetim adına risk tutumlarını uygulama,

[74] The Institute of Internal Auditors-UK &Ireland, **Position Statement-The Role of Internal Audit in Enterprise Wide Risk Management,** The Institute of Internal Auditors-UK &Ireland, September 2004, ss. 1-2.

f. Risk yönetimi konusunda hesap verme.

Yukarıda maddeler halinde sıralanan görevler kısaca; şöyle özetlenebilir. KRY kapsamında temel iç denetim görevleri olarak sıralanan faaliyetler iç denetim biriminin güvence hizmetleri çerçevesinde üstleneceği rolleri belirtmektedir. Şartlı olarak üstlenilebilecek görevler ise KRY sistemi olgunluk seviyesi ve üst yönetimin istekleri çerçevesinde iç denetim biriminin faaliyet çerçevesini çizmektedir. Son olarak iç denetim biriminin üstlenmemesi gereken görevler ise Sarbanes-Oxley yasası ve standartlarla paralellik göstermektedir. Yasaya göre sorumluluklar üst yönetimde bulunmalıdır[75]. İç denetimin risk yönetimi konusunda sorumluluk almaması gerektiği belirtilmekle beraber risk odaklı faaliyetler hakkında tarihi bir ilgi ve sorumluluğu olan[76] ayrıca risk yönetimi faaliyetleri hakkında hem üst yönetime hem de hissedarlara ve kamuya güvence veren bir birimin hiçbir sorumluluk üstlenmemesi kendi içinde bir çelişkiyi barındırmaktadır.

İç Denetim Enstitüsü tarafından yayınlanan raporda temel görevler, şartlı olarak üstlenilebilecek ve üstlenilmemesi gereken görevler şeklinde yapılan sınıflandırmaya ek olarak iç denetim birimi; kurum içinde geleneksel risk yönetimi ve kurumsal risk yönetimini savunanlar arasındaki çatışmaların yatıştırılmasında, çalışanların kurumsal risk yönetimi konusunda eğitimi sürecinde, operasyon yöneticilerine risk tanımlama sürecinde bilgi sağlama ve en iyi KRY uygulamaları hakkında bilgi temin etme sürecinde aktif olarak rol alabilir[77].

İç denetim standartlarında ve İç Denetim Enstitüsü tarafından yayınlanan raporda belirtilen iç denetim biriminin kurumsal risk yönetimi sürecindeki rolü aynı zamanda kurumun faaliyette bulunduğu sektöre, kurumun ve denetim departmanının büyüklüğüne, kurumun Sarbanes-Oxley yasasına uyum zorunluluğuna ve faaliyette bulunulan ülkenin yasal gerekliliklerine bağlı olarak değişebilir[78].

Bir diğer önemli noktada iç denetim birimi tarafından aynı alanlar için güvence ve danışmanlık faaliyetlerinin verilmesidir. Güvence ve danışmanlık gibi iki

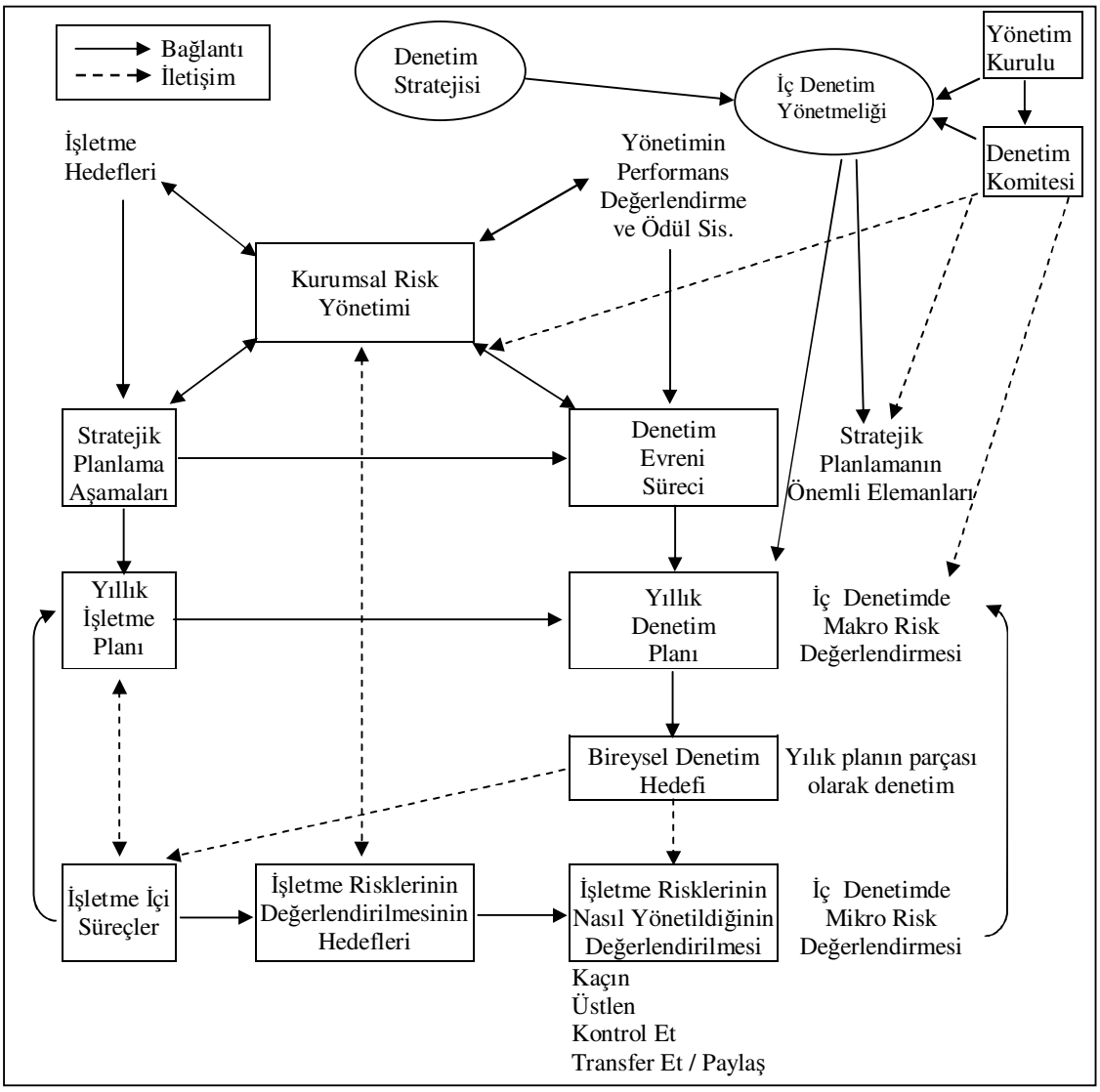
[75] Sarbanes Oxley Act Title III., Corporate Responsibility.
[76] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 34.
[77] Institute of Management Accountants, Statements of Management Accounting, **Enterprise Risk Management: Frameworks, Elements, and Integration,** Institute of Management Accountants, USA, 2006, ss 8-9.
[78] Gramling Audrey A. and Myers Patricia M., "Internal Auditing's Role in ERM", **Internal Auditor,** April 2006, s. 56.

uç fonksiyonun kurum içinde bir birim tarafından yerine getirilmesinin bağımsızlık ve objektiflik ilkesini zedeleyip zedelemediği tartışma konusudur.

Zaman içinde denetimin risk algılaması finansal ve uyumluluk risklerinden kurumun amaçlarına ulaşmasını engelleyecek bütün riskleri kapsayacak şekilde genişlemiştir[79]. Bunun da en büyük gerekçesi değişen rekabet ortamı ve buna bağlı olarak değişen kurum faaliyetleri ve iç ortamı sonucu iç denetçinin kurum hedeflerine ulaşılması sürecinde öne çıkan danışmanlık ve güvence verme fonksiyonudur.

Yaşanan muhasebe skandalları, kurumların farklılaşan ihtiyaçları, denetim komitelerinin ve iç denetimin, organizasyonun genelindeki pozisyonunu ve risk yönetimi ile olan ilişkilerini değiştirmiştir. David McNamee ve Georges Selim tarafından 1999 yılında tasarlanan model[80], 2004 yılında COSO tarafından yayınlanan KRY çerçevesi dikkate alınarak güncelleştirilip geliştirilerek aşağıda ele alınmıştır. Doğal olarak organizasyon yapıları kurum kültürlerinden, kurumların faaliyette bulundukları sektörlerden ve yasal gereklerden etkilenerek her kurum ve ülke açısından farklılık arzedebilir.

[79] Gupta Parveen P., **Internal Audit Reengineering: Survey, Model and Best Practices,** The Institute of Internal Auditors Research Foundation, USA, 2001, s. 54.
[80] McNamee David ve Selim Georges, **"The Risk Management and Internal Auditing Relationship: Developing and Validating a Model",** International Journal of Auditing, 1999, Vol: 3, s. 171.



Şekil 5: Bütünleştirilmiş Risk Yönetimi ve İç Denetim

Kaynak: McNamee David ve Selim Georges, "The Risk Management and Internal Auditing Relationship: Developing and Validating a Model", **International Journal of Auditing,** 1999, Vol: 3, s. 171'den alınarak güncelleştirilip geliştirilmiştir.

Risk yönetimi ve iç denetim kurum yönetiminin temel sorumluluklarından biridir. İşletmenin hedeflerine ulaşabilmesi için, yönetimin kurum içinde etkin işleyen risk yönetimi süreçlerinin bulunmasını ve kullanılmasını sağlaması gerekir. Denetim komitesi ve yönetim kurulu, uygun risk yönetimi süreçlerinin bulunup bulunmadığını ve bu süreçlerin yeterli ve etkin olup olmadığını belirlemek konusunda denetleyici bir rol oynar[81].

[81] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2100-4.

Bütünleştirilmiş risk yönetimi ve iç denetim sisteminin en temel öğelerinden birisi denetim komitesidir. İç denetim enstitüsü tarafından "kurumun denetim ve kontrol işlevlerinin gözetim ve denetiminden sorumlu bir komite[82]" olarak tanımlanan ve icracı olmayan üyelerden oluşan denetim komitesi üyelerinden en az bir tanesi finansal uzman olmalıdır[83].

Kurumsal yönetim ilkeleri çerçevesinde kurumlarda sorumluluk alanlarında boşluklar oluşmaması için genellikle birimlerin ve komitelerin yönetmeliklerinin bulunması gerekmektedir. Bu çerçevede daha önce ele alınan iç denetim yönetmeliğine benzer bir yönetmelik de denetim komitesi için geçerlidir.

Yıllık faaliyet raporunun bir parçası olarak yayınlanabilecek denetim komitesi yönetmeliğinde, komitenin sorumluluk çerçevesi çizilir. Sarbanes-Oxley yasası çerçevesinde, yasaya tabi şirketler için, hazırlanacak bu yönetmelik de risklerle ilgili olarak, riskler ve belirsizliklerin tanımlanması, değerlendirilmesi ve yönetimi sorumluluğunun denetim komitesi ve yönetim kurulunda olduğuna ilişkin bir açıklama yer almalıdır[84].

Denetim komitesi yönetmeliğinin içeriğine ilişkin standartlaştırılmış bir uygulama olmamakla birlikte yönetmelikte genel olarak aşağıdaki ana başlıklar yer alabilir[85]:

- Komite üyelikleri,
- Komitenin çalışma prensipleri,
- Toplantı sıklıkları,
- Komitenin ana faaliyetleri,
    - Kurumsal yönetim,
    - Raporlama,
    - Denetim ve muhasebe,
- Hissedarlara raporlama,
- Dış denetçi ve iç denetçi ile ilişkiler,
- Komitenin temel sorumlulukları.

[82] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2060-2 ve 1., Sarbanes Oxley Act Title III., Corporate Responsibility.
[83] Sarbanes Oxley Act Title III., Corporate Responsibility.
[84] Moeller Robert, **Sarbanes-Oxley and the New Internal Auditing Rules,** John Wiley & Sons, USA, 2004, s. 60., Moeller, **Brink's Modern Internal Auditing,** s. 180.
[85] Michael Baker Corporation Charter – Audit Committee, 19.02.2004.

Denetim komitesi, KRY sisteminin varlığı ve uygulamada ne derece kullanıldığı, risk yönetim sisteminin kurum amaçlarına ulaşılmasına katkısı, iç denetim aşamalarının güvenilirliği ile iç denetimin KRY sisteminin gelişimine katkısı hakkında yeterli bilgiye sahip olmalıdır[86].

Bunların yanı sıra denetim komitesinin iç denetim üzerindeki sorumlulukları, iç denetim birim yöneticisinin atanması, iç denetim yönetmeliğinin ve iç denetim plan ve bütçelerinin onaylanması ile önemli denetim bulgularının gözden geçirilmesi şeklinde sıralanabilir[87].

Sarbanes-Oxley yasası çerçevesinde, iç denetim birim yöneticisi ve bağımsız denetçi ile birlikte finansal raporlama ve iç kontrol sisteminin yeterliliğini gözden geçirmesi gereken denetim komitesi[88]; aynı zamanda bağımsız denetim firması ile anlaşma yapılmasından, teklif edilen denetim planı ve bütçesinin onaylanmasından ve denetlenmiş finansal tabloların yayınlanmasından da sorumludur[89].

Denetim komitesinin sorumluluklarını yerine getirebilmesi iç denetim biriminin yürüttüğü faaliyetlere, hazırladığı raporlara ve bu raporların sonuçlarına ilişkin düzenli aralıklarla denetim komitesine rapor vermesine bağlıdır.

Sarbanes-Oxley yasası öncesinde denetim komitesi üyeleri bağımsız ve iç denetim alanında hazırlanmış özet raporlarla yetinirken yasayla birlikte sorumlulukların artmasına paralel olarak denetim komitesi üyelerinin ve üst düzey yöneticilerin faaliyet çerçevelerini ve sorumluluk alanlarını hem iç denetim hem de bağımsız denetim raporları belirlemektedir. Bu çerçevede sorumluluk üst yönetime aittir.

Bunun yanısıra iç denetim yönetmeliği kurum çapında bir denetim stratejisinin oluşturulmasına, nelerin (kapsam), kim tarafından (kaynak) ve nasıl (metodoloji) yapılacağını göstererek katkıda bulunur[90].

İşletme süreçleri ile denetim süreçlerinin paralel hale gelmesi denetçinin kuruma değer katma ve danışmanlık fonksiyonlarının artmasını sağlamıştır. Yıllık

---

[86] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 149., Moeller, **Brink's Modern Internal Auditing,** ss. 1.75-176.
[87] Moeller, **Brink's Modern Internal Auditing,** s. 180.
[88] Moeller, **Sarbanes-Oxley and the New Internal Auditing Rules,** s. 63.
[89] Moeller, **Brink's Modern Internal Auditing,** s. 186.
[90] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 522.

işletme planı ile iç denetim planı arasındaki bağlantı mevcut ve geleceğe ait risklerin denetim faaliyetlerinde dikkate alındığından emin olmak için yerleştirilmiştir[91].

Yıllık denetim planının hazırlanması için temel verilerin bir kısmı da kurumsal risk yönetimi sisteminden gelmektedir. Aynı zamanda kurumsal risk yönetimi bileşenlerinden ilki olan kurum hedeflerinin belirlenmesi aşaması, risk yönetimi ve stratejik planlama için temel adımdır.

Şekilden de görülebildiği gibi risk yönetimi sürecinin çıktıları iç denetçi ve bağımsız denetçi tarafından kullanılmaktadır. Öte yandan stratejik planlama ve yönetimde de risk yönetimi süreçlerinin ve risk yönetimi temelli denetimin çıktıları yoğun olarak kullanılmaktadır.

Yıllık işletme planı ve iç denetim planı arasındaki ilişkinin bir benzeri stratejik plan ve denetim evreni için de geçerlidir. Kurum stratejik planı denetim evrenine yön verir ve denetim evreni kurum stratejik planı öğelerini içerir[92]. Nihai olarak da yıllık iç denetim planı denetim evrenine uygun bir şekilde hazırlanır. Denetim evreni, 3. bölüm 4. kısımda ayrıntılı olarak incelenecektir.

Yönetimin sorumluluklarını yerine getirmeye yönelik bu gelişmeler ve denetim komitesi ile üst yönetime raporlama zorunlulukları kurumsal yönetimin daha etkin çalışmasını ve sonuç olarak işletme dışı ilgililerin daha nitelikli ve daha güvenilir bilgiye ulaşmalarını sağlar[93].

İç denetim biriminin kime raporlama yapacağı konusu iç denetçinin bağımsızlığı ile doğrudan ilişkilidir. İç denetim birimi fonksiyonel olarak denetim komitesine veya dengi bir birime raporlama yaparken yönetimsel olarak ise CEO'ya raporlama yapar[94].

Yıllık denetim planının risk yönetimi temelli yapılması diğer bir ifadeyle makro risk analizi; denetim önceliklerinin belirlenmesi, denetim kaynaklarının en riskli faaliyetlerden başlatılmasını hedeflerken, bireysel denetimlerde risk analizi yani mikro risk analizi ise denetlenen faaliyete ilişkin risklerin tanımlanması, mevcut

[91] McNamee and Selim, **Risk Management: Changing the Internal Auditor's Paradigm,** s. 4.
[92] **a.g.e.,** s. 4.
[93] Walker Paul L., Shenkir William G. and Barton Thomas L., "ERM in Practice", **Internal Auditor,** August 2003, s. 55.
[94] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 1110-2.

iç kontrollerin değerlendirilmesi, risklerin giderilmesine yönelik iç kontrol uygulamalarının geliştirilmesini kapsar[95]. Yıllık denetim planına etki eden risk analizi sonuçlarının denetim komitesiyle paylaşılması-komitenin görüşünün alınması, ileride risk sıralaması veya planlamada dikkate alınmayan risklerden kaynaklanacak sorunları minimize eder.

İç denetçiler, yönetimin uyguladığı risk yönetim süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler önererek hem yönetime hem de denetim komitesine yardımcı olmalıdır. Kurumun risk yönetimi ve kontrol süreçlerinden yönetim, denetim komitesi ve yönetim kurulu sorumludur. Ancak danışmanlık rolünü üstlenen iç denetçiler de, bu risklerin tanımlanması, değerlendirilmesi ve risk yönetimi yöntemlerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilirler[96].

Uygulamada Kurumsal Risk Yönetimi komitelerinin oluşturulduğu da görülmektedir. Genellikle denetim komitesine bağlı olarak çalışan bu komitelerin çoğunlukla kurumsal risk yönetimi sistemini kurma aşamasında olan kurumlarda mevcut olduğu dikkat çekmektedir[97].

1.4. İÇ DENETİM VE RİSK YÖNETİMİNİN TÜRK MEVZUATI İÇİNDEKİ YERİ

Türk mevzuatında kurumsal yönetim ve iç denetim alanında yapılan düzenlemeler, 2000'li yılların başında yaşanan muhasebe skandallarının ayrıca Avrupa Birliği müzakere sürecinde bulunan bir ülkenin çabalarının izlerini taşımaktadır.

2003 yılında 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, ilki 2003 ve güncelleştirilmiş son hali 2005 yılında yayınlanmış olan Kurumsal Yönetim İlkeleri, Kasım 2005'te yayınlanan Bankacılık Kanunu ve halen tasarı halinde TBMM'de bulunan Türk Ticaret Kanunu Taslağı Türk mevzuatının uluslararası

[95] Özbek Coşkun, "İç Denetim Uygulamaları", **T.C. Maliye Bakanlığı Twinning Projesi,** İstanbul, 2005.
[96] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2110-1.
[97] Walker Paul L., Shenkir William G. and Barton Thomas L., **Enterprise Risk Management: Pulling it all Together,** The Institute of Internal Auditors Research Foundation, USA, 2002, s. 19.

düzenlemelere ve standartlara yaklaştırılması konusunda yapılan çalışmaların başlıcalarıdır.

Türkiye'de yürürlüğe konan ve halen tasarı halinde bulunan düzenlemeler üzerinde Enron skandalı sonrası süreçte yaşanan sıkıntıların ve özellikle Amerika'da yapılan düzenlemelerin, somut olarak Sarbanes Oxley Yasası'nın, etkileri gözardı edilemez.

1.4.1. 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu

Uluslararası standart ve Avrupa Birliği mevzuatına uyum çerçevesinde Aralık 2003'de 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kabul edilmiş[98] ve 1 Ocak 2006 tarihi itibariyle yürürlüğe girmiştir. Yürürlüğe girdiği şekliyle kanun Avrupa Birliği müktesebatına paraleldir. Müktesebatın 32 numaralı başlığı olan Finansal Kontrol; Kamu İç Mali Kontrol Sistemi, Dış Denetim ve AB Fonlarının Korunması alt başlıklarından oluşmaktadır[99].

5018 sayılı kanunun 5. kısmı İç Kontrol Sistemi başlığını taşımakta ve iç kontrol ve iç denetime ilişkin düzenlemeleri içermektedir. İlgili kanunun 55. maddesi iç kontrolün tanımı, 56. maddesi iç kontrolün amacı ve 63, 64, 65, 66 ve 67. maddeleri iç denetim, iç denetçinin görevleri, iç denetçinin nitelikleri ve atanması, İç Denetim Koordinasyon Kurulu ve İç Denetim Koordinasyon Kurulunun görevleri başlıklarından oluşmaktadır.

5018 sayılı kanunda Uluslararası İç Denetim Enstitüsü tarafından yapılan tanıma benzer bir iç denetim tanımı yapılmış ve uluslararası uygulamaya paralel olarak iç denetim "idarelerin yönetim ve kontrol yapıları ile mali işlemlerinin risk yönetimi, yönetim ve kontrol süreçlerinin etkinliğini değerlendirme[100]" faaliyetlerinden sorumlu tutulmuştur.

Bu kanunla birlikte kamu yönetimi bağlamında iç denetim gelecek hedefli, riskleri daha fazla dikkate alan, risk yönetimi süreçlerinin değerlendirilmesi faaliyetini kapsayan ve risk odaklı denetimden risk yönetimi temelli denetime geçişin ilk adımlarını atan bir niteliktedir.

---

[98] TBMM, **Kamu Mali Yönetimi ve Kontrol Kanunu**, 24.12.2003 tarih ve 25326 sayılı Resmi Gazete.
[99] Country Session: The Republic of Turkey, **Screening Chapter 32: Financial Control**, 30 June 2006, http://www.abgs.gov.tr/index.php?p=190&l=1 (18.07.2007)
[100] TBMM, **Kamu Mali Yönetimi ve Kontrol Kanunu**, Madde 63.

İç denetçinin görevlerinin ayrıntılı olarak ifade edildiği 64. madde "nesnel risk analizlerine dayanarak kamu idarelerinin yönetim ve kontrol yapılarını değerlendirme" ifade edilerek kamuda risk yönetimi temelli iç denetim sistemine geçiş yapıldığı fark edilmektedir. Bu görev tanımı risklerin belirlenmesi ve risk yönetimi süreçlerine iç denetçinin olası desteğini ifade etmektedir.

Kanunun 65. maddesinde iç denetçinin nitelikleri ve atanma kriterlerinden bahsedilmiştir. Kanunda dikkat çeken nokta iç denetçilerin bağımsızlığına yapılan vurgudur. Fakat kanunda yer aldığı şekliyle "iç denetçiler, raporlarını doğrudan üst yöneticiye sunar" ifadesi uluslararası standartta yer alan idari ve fonksiyonel raporlama sınıflandırmasına uygun değildir. Bu haliyle bağımsızlık kriterinin uygulamada tam anlamıyla kabul görmemesi olasıdır. Bu tür bir raporlama idari raporlamaya dahildir ve bunun yanısıra bir de fonksiyonel raporlama yapılmalıdır.

Ayrıca, "kamu idarelerinin iç denetim sistemlerini izlemek, bağımsız ve tarafsız bir organ olarak hizmet vermek" amacıyla İç Denetim Koordinasyon Kurulu oluşturulmuş ve kurulun görevleri kanunda sıralanmıştır[101]. Bu kurul kanunda sıralanan görev çerçevesi ve amaçları itibariyle Uluslararası İç Denetim Enstitüsü'nü anımsatır bir yapıdadır. Ayrıca bu kurul tarafından Kasım 2006 tarihinde "Kamu İç Denetim Standartları ve Kamu İç Denetçileri Meslek Ahlak Kuralları" yayınlanmıştır.

Bu kanunun 65. Maddesine dayanılarak "İç Denetçiler Çalışma Usul ve Esasları Hakkında Yönetmelik[102]" yayınlanmıştır. Bu yönetmeliğin 5. maddesinde "iç denetim, nesnel güvence sağlamanın yanında, özellikle risk yönetimi, kontrol ve yönetim süreçlerini geliştirmede idarelere yardımcı olmak üzere bağımsız ve tarafsız bir danışmanlık hizmeti sağlar" şeklinde bir iç denetim tanımı yapılmıştır. Bu tanım uluslararası iç denetim standartlarına paraleldir.

Sözkonusu yönetmeliğin 37. maddesinde risklerin tanımlanması ve gerekli stratejilerin geliştirilmesinden yönetim sorumlu tutulmaktadır. Yine yönetmeliğin 36. maddesinde de tanımlanan risklerin değerlendirilip sıralanarak denetimin planlanması aşamasında kullanılması gerekliliğinden bahsedilmekte ve bu veriler ışığında denetim programının hazırlanması öngörülmektedir.

---

[101] TBMM, **Kamu Mali Yönetimi ve Kontrol Kanunu**, Madde 67.

[102] Maliye Bakanlığı, **"İç Denetçiler Çalışma Usul ve Esasları Hakkında Yönetmelik",** 12.07.2006 tarih ve 26226 sayılı Resmi Gazete.

1.4.2. SPK Düzenlemeleri

Sermaye Piyasası Kurulu tarafından yapılan, doğrudan iç denetime veya iç kontrole yönelik herhangi bir düzenleme yoktur. Bununla beraber 2006 Haziran ayında yürürlüğe giren Bağımsız Denetim Standartları 27. kısım "Bağımsız Denetimde İç Denetim Çalışmalarından Yararlanılması[103]" başlığı altında; bağımsız denetçinin çalışmaları esnasında kurum iç denetim ve iç kontrol sisteminden yararlanabilmesi için kurum iç kontrol sisteminin incelenmesi gerekliliğinden bahsedilmektedir.

SPK, Kurumsal Yönetim İlkelerinin ilk halini Temmuz 2003'de düzeltilmiş son şeklini de Şubat 2005'te yayınlanmıştır. Sözü edilen ilkelerin "Kamuyu Aydınlatma ve Şeffaflık" bölümü 1.6. numaralı kısmında kurumsal yönetim uyum raporu ve yıllık faaliyet raporlarından söz edilmektedir[104].

Yıllık faaliyet raporunda bir bölüm olarak da yer alması gereken kurumsal yönetim uyum raporunda bu çalışmanın da kapsamına giren; risk yönetimi ve iç kontrol mekanizması, yönetim kurulunda oluşturulan komitelerin sayı, yapı ve bağımsızlığı başlıkları yer almaktadır. Kamunun aydınlatılması kapsamında gerekli kurum bilgilerinin bu başlıklar altında açıklanması uygun görülmektedir.

Risk yönetimi ve iç kontrol mekanizması başlığı altında kurumda mevcut iç kontrol ve risk yönetimi uygulamaları hakkında bilgiler yer almalıdır. Burada henüz iç kontrol ve risk yönetimi sistemi oluşturulmamışsa gerekçeleriyle açıklanmalıdır. Ayrıca kurum içinde iç denetim biriminin raporlama yapacağı taraflar, son dönemde dikkate alınan risk türleri ve güncel gelişmelerin aktarılması son olarak da iç denetim birimi tarafından kullanılan bilgisayar yazılımlarından bu kısımda bahsedilebilmektedir.

Yönetim kurulunda oluşturulan komitelerin sayı, yapı ve bağımsızlığı başlığı altında ise denetimden sorumlu komitenin üye sayıları, toplantı sıklıkları, görev alanları ve sorumlulukları hakkında bilgiler yer almaktadır. Ayrıca varsa risk yönetimi ve kurumsal yönetim komitesi gibi diğer üst düzey komiteler, hakkında da bilgiler bu başlık altında yer almaktadır.

---

[103] Sermaye Piyasası Kurulu, **Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ,** Seri: X, No: 22, 12.06.2006 tarih ve 26196 sayılı Resmi Gazete, 27. Kısım.
[104] Sermaye Piyasası Kurulu, **Kurumsal Yönetim İlkeleri,** Şubat 2005, s, 22.

1.4.3. Bankacılık Kanunu

Kasım 2005'te yürürlüğe giren Bankacılık Kanunu'nun[105] üçüncü kısmı Kurumsal Yönetim olarak adlandırılmıştır. Bu kısımda iç kontrol ve iç denetim sistemleri ayrıntılı olarak ele alınmış fakat iç denetim ve risk yönetiminin ortak çalışma alanlarına ve her iki sistem arasında gerçekleşebilecek olası veri transferlerine değinilmemiştir.

Kanunda yer almayan ve yukarıda sözü edilen düzenlemelere 1 Kasım 2006 tarihinde yayınlanan "Bankaların İç Sistemleri Hakkında Yönetmelik" üçüncü kısım "İç Denetim Sistemi" başlığı altında yer verilmiştir. Sözkonusu yönetmelikte iç denetim sisteminin amacı "iç kontrol ve risk yönetimi sistemlerinin etkinliği ve yeterliliği hakkında güvence sağlamak[106]" şeklinde ifade edilmiştir. Dönemsel değerlendirmelerin riske dayalı olması gerektiği belirtilmekle beraber, banka tarafından kullanılan risk yönetimi tekniklerinin denetlenmesi gerektiği yönetmelikte vurgulanmaktadır.

Yönetmelikte aynı zamanda risk yönetimi süreçlerinin de iç denetçi tarafından denetleneceği; 21. madde 4. fıkra "risk ölçüm modelleriyle ilgili denetimler gerçekleştirilir" hükmünden anlaşılmaktadır. Bu durum KRY temelli çalışan bir iç denetim sistemi için olumlu bir adımdır ve uluslararası uygulamaya paraleldir.

Yönetmeliğin 26. Maddesi "Riske Dayalı Denetim" başlığı altında; bankanın maruz kaldığı risklerin iç denetçi tarafından değerlendirilmesinin amacı; denetim çalışmalarında öncelik verilecek alanların belirlenmesi, denetim kapsamı ve sıklığının belirlenmesi olarak açıklanmıştır. Ayrıca risk değerlemesine ilişkin hususlar sıralanarak risk tanımlamaları ve risk değerlemelerinin önemi vurgulanmıştır. Bu süreçte iç denetçinin odaklanması gereken başlıca alanın risk tanımlamaları ve risk değerlemeleri olduğu yönetmelikten anlaşılmaktadır.

Kamunun aydınlatılması kapsamında ele alınması gereken bir diğer husus da faaliyet raporlarıdır. Kurumsal yönetim ilkeleri çerçevesinde bankalar tarafından

[105] TBMM, Bankacılık Kanunu, 01.11.2005 tarih ve 25983 sayılı Resmi Gazete.
[106] Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankaların İç Sistemleri Hakkında Yönetmelik",** 01.11.2006 tarih ve 26333 sayılı Resmi Gazete, Madde 21.

hazırlanması gereken yıllık faaliyet raporları hakkında yönetmelik 1 Kasım 2006 tarihinde yayınlanmıştır[107]. Yönetmelik çerçevesinde bankalar;

- Denetim komitesinin iç kontrol, iç denetim ve risk yönetim sistemlerinin işleyişine ilişkin değerlendirmeleri ve hesap dönemi içerisindeki faaliyetleri hakkında,
- Denetim komitesi üyeleri, toplantı sıklıkları, bağımsızlıkları ve bağımsız denetçinin seçimi sürecine ilişkin,
- Risk türleri itibariyle uygulanan risk yönetimi politikalarına ilişkin,

bilgileri içerecek şekilde hazırladıkları faaliyet raporunu bağımsız denetçinin olurunu aldıktan sonra izleyen dönemin Mayıs ayı sonuna kadar yayınlamak zorundadırlar.

Kurumsal yönetim ilkeleri çerçevesinde faaliyet raporları ve kurumsal uyumluluk raporlarının kamuoyu ile paylaşılması, karşılaştırılabilir olması açısından belli bir tekdüzelikte hazırlanması çok önemlidir. Ayrıca bu raporların öngörülen zamanlarda yayınlanması halinde anılan düzenlemelerin beklenen faydalara ulaştıracağı açıktır.

1.4.4. Yeni Türk Ticaret Kanunu Tasarısı

Yeni Türk Ticaret Kanunu Tasarısı; Kurumsal Yönetim İlkeleri, denetim komitesi, uluslararası muhasebe standartları ve iç denetim gibi bir takım çağdaş düzenlemeleri kapsamaktadır. Tüm bu yenilikler aynı zamanda bir kurumsal yönetim ilkesi olan şeffaflık kapsamında ele alınabilir. Tasarıda iç denetim çok az yer kaplamakla beraber kabulleri bakımından uluslararası uygulama ve iç denetim standartları ile paralellik arz etmesi olumlu bir adımdır.

Yeni Türk Ticaret Kanunu tasarısında çağdaş anlamda "iç denetim" iki yerde geçmektedir. Bunlardan ilki Kurumsal Yönetim başlığı altında yer almakta olup kurumda iç denetim görevini yerine getiren Yönetim Kurulu üyelerinin sahip olmaları gereken haklardan bahsedilmektedir[108].

---

[107] Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankalarca Yıllık Faaliyet Raporlarının Hazırlanmasına ve Yayımlanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik",** 01.11.2006 tarih ve 26333 sayılı Resmi Gazete.

[108] T.C. Adalet Bakanlığı Türk Ticaret Kanunu Komisyonu, **Yeni Türk Ticaret Kanunu Tasarısı,** 24.02.2005, Genel Gerekçe Madde 090.

İkinci olarak iç denetim II. Kitap: Ticaret Şirketleri, Dördüncü Kısım: Anonim Şirketler, II. Bölüm: Yönetim Kurulu başlığı altında yer almaktadır. Bu kısımda bağımsız dış denetim ihtiyacının yanısıra iç denetim faaliyetinin de artık bir zorunluluk haline geldiğinden bahsedilmekte ve bu durumun Kurumsal Yönetim İlkelerinden kaynaklandığına vurgu yapılmaktadır[109].

İç denetimin yanısıra iç kontrole yönelik düzenlemeler tasarıda Madde 378'de "Pay senetleri borsada işlem gören şirketlerde, yönetim kurulu, şirketlerin varlığını, gelişmesini ve devamını tehlikeye düşüren sebeplerin erken teşhisi ve bunun için gerekli önlem ve çarelerin uygulanması amacıyla, uzman bir komite kurmak, sistemi çalıştırmak ve geliştirmekle yükümlüdür."şeklinde yer almıştır.

Ayrıca tasarının 397. Madde 2. Bendinde yıllık raporların da bağımsız denetimden geçirilme zorunluluğu yer almaktadır. Bu madde kurumsal yönetim ilkeleri çerçevesinde atılmış bir diğer önemli adımdır. Çünkü işletme içi veya dışı ilgililerin, işletme faaliyetleri hakkında standart formatta bilgi alabileceği belgelerden birisi de yıllık faaliyet raporlarıdır. Bu çerçevede yıllık raporlarının denetlenmesi son derece önemlidir.

Yasa tasarısının 398. Madde 2. Bent C. Fıkrasında yer alan "Yıllık rapor ile diğer raporlarda gelecekteki gelişime ilişkin risklerin gereği gibi ifade edilip edilmediği de açıklanır" hükmü ile bağımsız denetçinin sorumluluk alanına, raporlarda risklere ilişkin bir takım açıklamaların yer alıp almadığına ilişkin değerlendirme yapma zorunluluğu da eklenmiştir.

Tasarının yasalaşmasını izleyen süreçte ilgili kurumların çıkaracakları yönetmeliklerle, dikkate alınacak riskler, ölçüm yöntemleri ve diğer hususlar ayrıntılı bir şekilde düzenlenmelidir.

[109] **a.g.e.,** Madde 375.

II. BÖLÜM
KURUMSAL RİSK YÖNETİMİ

Ekonomik krizler ve muhasebe-denetim skandalları ile birlikte piyasa mekanizmasına ve şirketlerin verilerine olan güvenin sarsılması bütünsel olarak risklerin tanımlanıp, değerlendirildiği ve sonuç olarak da riskler karşısında gerekli önlemlerin alındığı bir risk yönetimi sisteminin ön plana çıkmasına zemin hazırlamıştır.

2.1. GELENEKSEL RİSK YÖNETİMİ YAKLAŞIMINDAN KURUMSAL RİSK YÖNETİMİ YAKLAŞIMINA UZANAN SÜREÇ

Risk odaklı faaliyetler ile başlayan risk yönetimi sürecinin olgunlaşması Geleneksel Risk Yönetimini ortaya çıkarmış ve ardından işletmelerin ihtiyaçları ve piyasa mekanizması Kurumsal Risk Yönetimi'nin (KRY) (Enterprise Risk Management-ERM) gelişiminde temel rolü oynamıştır. Risk odaklı faaliyetler, Geleneksel Risk Yönetimi ve Kurumsal Risk Yönetimi arasındaki benzerlikler ve temel farklılıklar risk yönetiminde perspektif, odak nokta, sorumlular, ayrıntı seviyesi, zamanlama, dil, raporlama, kontrol odağı, araçlar, amaç, kapsam, standartlar, vizyon ve sisteme yön verenler başlıkları altında Tablo 3 yardımıyla ele alınacak ve açıklanacaktır.

Risk odaklı faaliyetlerin temeli, COSO tarafından 1992 yılında yayınlanan "İç Kontrol Çerçevesi"nin risk değerleme aşamasına dayanmaktadır. Risk odaklı faaliyetler, risk yönetimi ve kurumsal risk yönetimi de karşılaştırmalı olarak izleyen tabloda ele alınmaktadır[110].

[110] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 76.

Tablo 3: Risk Odaklı Faaliyetlerden Kurumsal Risk Yönetimine Uzanan Süreç

Faktör	Risk Odaklı Faaliyetler	Geleneksel Risk Yönetimi	Kurumsal Risk Yönetimi
Perspektif	Fiziksel tehditler	Tüm tehditler	Fırsatlar ve tehditler
Odak	Özel projeler	Özel faaliyetler	Kurum geneli ve kurum ortakları temelli
Yürütücüler (Sorumlular)	Uzmanlar	Yöneticiler	Tüm çalışanlar
Ayrıntı Seviyesi	Karmaşık analizler	Detaylı analizler	Genel değerlendirmeler
Zamanlama	Bir kez	Düzenli	Sürekli
Dil	Farklı terimler	Benzer terimler fakat farklı açılar	Genel dil ve perspektif
Raporlama	Bir kez detaylı raporlama	Yüksek seviyede fakat parçalanmış raporlar	Bütünleştirilmiş işletme raporlaması
Kontrol Odağı	Güvenlik ve olasılık planlaması temelli	Bireysel kontrol mekanizmaları temelli	Kontrol çerçeveleri temelli
Araçlar	Veri analizi	Kontrol-Risk Öz Değerlendirme (KRÖD) ve anketler	(KRÖD) ve anketler ve KRY'nin işletme süreçleri ile bütünleştirilmesine yönelik diğer araçlar
Amaç	Düşük seviyede güvence	Risk kayıtlaması için risk tanımlamaları ve yönetimi	Kurum amaçlarına ulaşılması
Kapsam	Uygunluk	Operasyonel	Stratejik
Standartlar	Uzmana bağımlı	Yöneticiye bağımlı	Kurum risk politikasına bağımlı
Vizyon	Kurum kaynaklarının korunması	Yönetim kurulu ve yöneticilerin korunması	Bütünleştirilmiş risk yönetimi çerçevesi oluşturulması ve kurum itibarının iyileştirilmesi
Sisteme Yön Verenler	Dış tehditler	CEO ve Risk Yönetimi Müdürü	Pay sahipleri, CEO ve Risk Yönetimi Müdürü

Kaynak: Spencer Pickett K. H., **Auditing The Risk Management Process,** John Wiley & Sons, USA, 2005, s. 76-77., McNamee David ve Selim Georges, **Risk Management: Changing the Internal Auditor's Paradigm,** The Institute of Internal Auditors, USA, 1998, s. 5.

Risk yönetimi iç kontrol sistemi temelli bir oluşumdur. Bunun da temelinde bireysel hatalardan kaynaklandığı düşünülen riskleri-fiziksel tehditleri kontrol faaliyetleri aracılığıyla önlemek ve etkisini azaltmak düşüncesi yani risk odaklı faaliyetler vardır. Zamanla değişen risk algılaması risklerin sadece bireysel hatalardan değil, işletme stratejilerinden ve iç ve dış ortamdan kaynaklanabileceğini

ve risklerin fırsatları da içerdiği gerçeğinin kabulünü sağlamıştır. Bu kabul KRY'nin de temelini oluşturur.

Risk odaklı faaliyetlerin temelinde fiziksel tehditler varken geleneksel risk yönetimi yaklaşımının temelinde kurumu ilgilendiren bütün tehlikeler-tehditler yer almaktadır. Kurumsal risk yönetiminde ise, riskler sadece tehlike-tehdit boyutuyla ele alınmamakta aynı zamanda fırsatlar açısından da değerlendirilmektedir[111]. Farklılaşan bu risk tutumu sonucunda risk yatıştırması yerini risk optimizasyonuna bırakmakta ve böylelikle kurum açısından daha fazla katma değer oluşturulmaktadır.

Geleneksel yaklaşımda risk sorumlulukları dağıtılır. Sorumlulukların fonksiyon bazlı dağıtılması risk yönetimi süreçlerinin ve raporlamaların kurum çapında bir bütün olarak çalışmasını engeller. Bu açığı kapatmak için kurumsal risk yönetimi, sorumlulukların dağıtılmadığı, belli bir hiyerarşi içinde uygulamaların gerçekleştirildiği ve raporlamaların KRY komitesine yapıldığı bir sistem şeklinde tasarlanmıştır[112]. Aynı zamanda bu yapılanma SOX (Sarbanes Oxley) çerçevesinde, risk yönetiminin sorumluluğunun üst yönetimde olması gerekliliğine de uygundur.

Geleneksel yaklaşımda risk sorumluluklarının dağıtılması bu görev dağılımının içinde yer almayan çalışanlar açısından risklere karşı bir ilgisizliğe neden olmaktadır. Bu sakıncalı durumu ortadan kaldırmak için kurumsal risk yönetimi yaklaşımında sorumluluk alanları kaldırılarak "riskler bütün çalışanların ilgi ve sorumluluk alanına dahildir" ilkesi yaygınlaştırılmaya çalışılmıştır.

Geleneksel yaklaşımda, ele alınan spesifik riskler; kendi terminolojileri, kendi risk çevirimleri içinde değerlendirilmekte, ayrı ayrı raporlanmakta ve riskler farklı risklerden izole edilmekte yani "depo risk faaliyeti" temelli çalışmaktadır. Bu tercih kurum genelinde ortak bir risk dili, raporlaması ve ortak bir risk kültürü oluşmasını engellemektedir[113]. Depo temelli risk yönetimi geçmişin daha az karmaşık çevre koşullarında etkin çalışmıştır. Fakat günümüzün karmaşık, coğrafi olarak genişlemiş

[111] Chapman Christy, "The Big Picture – Enterprise Risk Management Services", **Internal Auditor,** June 2001, s. 33.
[112] Banham, "Enterprising Views of Risk Management", s. 67.
[113] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 71.

kurum yapılarında ve üretici ve tüketicilerle bütünleşmenin yüksek seviyelere ulaştığı koşullarda etkinliğini yitirmiştir[114].

KRY portföy yaklaşımı temelli çalışmakta ve böylelikle farklı kategorilerdeki spesifik risklere odaklanmak yerine yüksek riskli alanlara odaklanmaktadır. Portföy yaklaşımında riskler öncelikle gruplanır, gruplar kendi içinde yükselen ve düşen risklere sahip olabilir. Gruplararası karşılaştırmadan sonra, grupların etkileri dikkate alınarak, kritik riskler belirlenir ve bunlara ilişkin gerekli önlemler alınır[115]. Bu sayede risklerin etkisini azaltmak için tutulması gereken sermaye miktarı optimum seviyede tahmin edilebilmektedir[116]. Portföy yönetimi temelli çalışan KRY sayesinde işletme genelinde ortak dil kullanılmaya başlanmış ve raporlama da geleneksel risk yönetiminden farklı olarak işletme genelinde yapılır hale gelmiştir.

Geleneksel risk yönetimi sürecinde riskler tanımlanmakta, sınıflandırılmakta ve değerlendirilmektedir fakat bu bilgilerin faaliyetlere nasıl dönüştürüleceği ve kuruma nasıl değer katacağı hususu pek dikkate alınmaz[117]. Geleneksel yaklaşım sözkonusu faaliyetleri Kontrol-Risk Öz Değerlendirme teknikleri ve anketler aracılığıyla gerçekleştirmektedir.

Kurumsal yaklaşım da ise riskler bütün kurum çapında ve farklı risk sınıflamalarında değerlendirilip, tek bir risk yönetim biriminde sonuçları toplanarak risk raporlamasında ve risk tutumlarında birlik sağlanmaktadır. Sözkonusu faaliyetler Kontrol-Risk Öz Değerlendirme teknikleri ve anketlerin yanısıra KRY ve işletme süreçlerinin bütünleştirilmesine yönelik diğer araçları da kullanmaktadır.

Kapsam bakımından risk odaklı faaliyetler uygunluk faaliyetlerine odaklanmıştır. Geleneksel risk yönetimi ise finansal ve tehlike risklerine odaklanırken kurumsal risk yönetimi bu risklerin yanısıra operasyonel ve stratejik risklerle de ilgilenmektedir[118].

---

[114] Deloitte Touche Tohmatsu, **Managing Business Risks,** 2005, http://www.deloitte.com/growth, 20.02.2005, s. 5.
[115] Chapman, "The Big Picture – Enterprise Risk Management Services", s. 32.
[116] Banham Russ, "Enterprising Views of Risk Management", **Journal of Accountancy,** June 2004, s. 67.
[117] Chapman, "The Big Picture – Enterprise Risk Management Services", s. 33.
[118] Banham Russ, "Fear Factor: Sarbanes-Oxley offers one more reason to tackle enterprise risk management", **CFO Magazine,** June 2003, s. 1.

Amacı kurumun hedeflerine ulaşması sürecinde yönetim kurulu ve üst yönetime yardım etmek olan iç denetim birimi açısından risklerin kurum çapında ele alınıp değerlendirmesi önemlidir ve bu yüzden KRY tercih nedenidir[119].

Risk sınıflandırmaları ve risk tutumlarının değişimi denetçi yeterliliklerinin değişmesine neden olmuştur. Geleneksel denetimde denetçinin muhasebe bilgisine sahip olması yeterliyken artık muhasebe bilgisine ek olarak stratejik planlama, süreç yapılanması, pazarlama ve hatta bilgi işlem teknolojileri bilgisine sahip denetçilere ihtiyaç duyulmaktadır[120].

Genel olarak karşılaştırılan bu sistemlerin vizyonları ise kurum kaynaklarının korunması sürecinden kurum itibarının iyileştirilmesine kaymıştır. Kuşkusuz bu durum sisteme yön verenler açısından da farklılık göstermektedir. Risk odaklı faaliyetler dış tehditlere göre şekillenirken kurumsal risk yönetimi ise pay sahipleri, CEO ve risk yönetim müdürünün beklentileri doğrultusunda şekillenir.

2.2. KURUMSAL RİSK YÖNETİMİ

Kurumsal risk yönetimine ilgi, krizlerle birlikte artmış ve COSO tarafından 2006 yılında ayrıntılı bir rehber yayınlanmıştır. Bu çalışma ile birlikte küresel ölçekte standart olarak uygulanabilir bir rehber ortaya çıkmıştır.

2.2.1. Kurumsal Risk Yönetimi Kavramı ve Kurumsal Risk Yönetimi Çerçevesi

İster kâr amacı güden ister gütmeyen bir kurum olsun bütün kurumlar faaliyetlerini belirsizlik ortamında yürütürler. Kurumların risk ve fırsatlarla karşılaşmasına neden olan belirsizlik, gelecekte olabilecek potansiyel olayların olasılıklarının ve bu olayların sonuçlarının belirlenememesi durumudur. Kuşkusuz belirsizlik ortamı kurumun stratejik tercihlerine bağlı olarak değişebilmektedir[121].

[119] The Institute of Internal Auditors, "Managing Risk from the Mailroom to the Boardroom", **Tone at the Top,** Issue 18, June 2003, s. 2.
[120] Banham, "Fear Factor: Sarbanes-Oxley offers one more reason to tackle enterprise risk management", s. 1.
[121] Committee of Sponsoring Organizations of the Treadway Commission, **COSO Enterprise Risk Management Framework (Draft),** s. 1.

Küresel ölçekte, risk yönetiminde başta COSO Kurumsal Risk Yönetimi çerçevesi olmak üzere genellikle finans sektörü tarafından kullanılan BASEL II Prensipleri ve Avustralya Risk Yönetimi Standartları bulunmaktadır.

Uluslararası İç Denetim Enstitüsü işbirliği ile Shannon, Margaret ve Karen tarafından, İç Denetim Enstitüsü'ne üye İç Denetim Birim yöneticileri üzerinde yapılan ve 2005 yılında tamamlanan araştırmanın "Hangi risk çerçevesini kullanmaktasınız ?" sorusuna verilen cevapların sıralaması 1. COSO KRY Çerçevesi (% 37), 2. Diğer (% 32), 3. Basel II (% 12), 4. Avustralya Standartları (% 4), 5. Belirsiz (% 4), 6. Kullanmayanlar (% 10) olarak belirlenmiştir. COSO KRY Çerçevesi % 37 ile en çok tercih edilen çerçeve olarak belirlenirken, araştırmaya katılanların % 32'si "Diğer" cevabını vermekle muhtemelen kurum içi geliştirilen bir risk çerçevesi kullandıklarını belirtmişlerdir. Diğer yandan Basel II'yi kullandıklarını belirtenlerin (% 12) büyük çoğunluğunun bankacılık sektöründe çalıştıkları belirlenmiştir. Araştırmaya katılanların % 4'ü Avustralya Standartlarını kullandıklarını % 10'u ise herhangi bir risk çerçevesi kullanmadıklarını belirtmişlerdir[122].

Yukarıda ifade edilen araştırma sonuçları bu çalışmada neden COSO Kurumsal Risk Yönetimi çerçevesinin tercih edildiğini açıklamaktadır. Bu bölümde ayrıntılı bir şekilde incelenen Kurumsal Risk Yönetimi Çerçevesi'nin üçüncü bölümde iç denetim fonksiyonu ile beraber çalışması ve bütünleştirilmesi ele alınmaktadır.

Kurumsal risk yönetimi, bir kurumun hedeflerine ulaşmasını etkileyebilecek potansiyel olayları tanımlayan, risk alma istekliliği sınırları içinde yöneten ve kurum hedeflerinin başarılması konusunda makul derecede güvence sağlayan, kurum genelinde yapılandırılmış ve kurum yönetim kurulundan, yönetimden ve diğer çalışanlardan etkilenen bir süreçtir[123].

KRY'nin ortaya çıkış gerekçesi risklerin de ortaya çıkış gerekçesi olan kurumun başarmayı hedeflediği stratejileri ve amaçlarıdır. KRY'nin temel amacı,

---

[122] Anderson Shannon W., Christ Margaret H. and Sedatole Karen L., **Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-Organizational Settings,** USA, January 2006, The Institute of Internal Auditors Research Foundation.
[123] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 6.

risklerin yönetilmesi sağlanarak kurum amaçlarına ulaşmak olarak ifade edilebilir[124]. Etkin bir şekilde çalışan ve amaçlarına ulaşan KRY sistemi de ancak etkin işleyen KRY temelli bir iç denetim sisteminin varlığı halinde mümkündür[125]. KRY'nin etkin çalışabilmesi ancak sistemin etkinliğinin denetlenmesi olası eksikliklerin ve aksayan yönlerin tespiti ve düzeltilmesi ile mümkündür. Kuşkusuz bu fonksiyon da kurum içinde bağımsız hareket edebilme yeterliliği olan iç denetim birimi tarafından gerçekleştirilmelidir.

KRY tanımının öne çıkan temel öğeleri aşağıdaki gibi sıralanabilir[126]:

- Sürekli ve akışkan bir süreçtir. KRY bir olay veya durumdan oluşan bir etkinlik değil kurum faaliyetlerinin içinde yer alan bir eylemler serisidir.
- Kurumun her seviyesindeki çalışanlardan etkilenir. Yönetim kurulu KRY'nin en önemli öğelerinden birisidir. Bunun yanısıra stratejileri, işlemleri ve politikaları onaylayan yöneticilerin de KRY üzerinde etkinlikleri fazladır.
- Kurumun her seviyesinde uygulanır. KRY kurum genelindeki faaliyetlerle ilgilidir. Bu faaliyetler kurum tepe yönetimi faaliyetleri, stratejik planlama ve kaynak tahsisi olabileceği gibi departman temelli faaliyetler de, pazarlama ve insan kaynakları da olabilir.
- Risklerin tamamıyla yatıştırılmasına gerek yoktur. Riskler risk alma istekliliği sınırları içinde yönetilir. Risk alma istekliliği, basit olarak, niteliksel - yüksek, orta ve düşük sınıflandırması şeklinde - veya niceliksel - büyüme ile ilgili hedeflerin yansıtılması – olarak düşünülebilir.
- KRY, kurum hedeflerinin başarılacağına ilişkin makul düzeyde güvence sağlar.

Makul düzeyde güvence, geleceğin belirsizliği ve risklerin gelecekle ilgili olmasından dolayı önceden kesin bir tahmin yapılamayacağı gerçeğine dayanır. Ayrıca insan doğasından kaynaklanabilecek hatalı risk değerleme ve risk tutumu kararı alma gibi nedenlerle KRY sistemi ne kadar iyi kurulursa kurulsun belli bir takım sınırları vardır[127].

---

[124] Sobel, **a.g.e,** s. 1.03.
[125] Sobel, **a.g.e,** ss. 3.03-3.10.
[126] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management – Integrated Framework (Executive Summary),** USA, 2004, s. 2.
[127] Moeller, **Brink's Modern Internal Auditing,** s. 111.

Hiçbir kurum risklerden arındırılmış bir ortamda faaliyetlerini yürütmediği gibi KRY'de hiçbir kuruma böyle bir ortamı sağlayamaz. Kuruma temel katkısı, risklerle dolu bir rekabet ortamında faaliyetlerin daha etkin yürütülmesi olan KRY'nin başlıca faydaları şu şekilde sıralanabilir[128]:

- Risk alma istekliliğine bağlı olarak da risk stratejilerini oluşturur ve böylelikle riskli alanlara kaynak tahsisi kolaylaşır.
- Risk ve getiri arasındaki ilişkiyi kuvvetlendirir. Kurumlar değer oluşturma veya mevcut değerlerini korumak adına riskleri kabul ederler ve bir getiri beklerler. KRY yürüttüğü faaliyetlerle risk ve getiri arasındaki ilişkiyi sağlamlaştırır.
- Kurum yönetiminin, risk tutumlarına ilişkin kararlar alabilmesi için uygun metotlar ve teknikler sağlar.

Bu sayede kurum üst yönetimi daha az belirsizlik daha çok belirlilik koşulları altında karar alır. Ayrıca alınan kararların uygun verilerle desteklenmesi üst yönetime performans savunmaları için fırsat verir.

- Kurumun daha az sürprizlerle karşılaşıp, hedeflerine ulaşma olasılığını artırır ve böylelikle olası maliyetleri ve zararları azaltır.
- Riskler karşısında bütün kurum düzeyinde ortak çalışılması gerektiğinin ve risklerin potansiyel domino etkilerinin anlaşılmasını sağlar.
- Risklerin izlenmesini ve kurum faaliyetlerine etkisinin ölçeklendirilmesini sağlar.
- Rasyonel sermaye gerekliliğinin belirlenmesine yardımcı olur. Riskler hakkında yönetime sağlanan bilginin kalitesi arttıkça yönetim de sermaye ihtiyacı değerlendirmesini daha etkin yapar.

Rasyonel sermaye gerekliliğinin belirlenmesi aşamasında risk değerleme fonksiyonunun önemi büyüktür. Rasyonel sermaye gerekliliğinin optimum tahmini, tutulması gereken net çalışma sermayesinin optimizasyonunu sağlayarak kurum açısından atıl sermaye tutulması önlenmiş olur.

---

[128] The Institute of Internal Auditors, UK & Ireland, **Position Statement-The Role of Internal Audit in Enterprise-Wide Risk Management,** s. 4., Funston Rick, "Creating a risk-intelligent organization", **Internal Auditor,** April 2003, s. 1., Matyjewicz and D'arcangelo, "ERM Based Auditing", ss. 8-9., Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** ss. 1-4., TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **Kurumsal Risk Yönetimi,** İstanbul, Aralık 2006, s. 53.

- Kurum hedeflerine ulaşılabilmesi açısından risk yönetim sisteminin sağlamlığı hakkında makul düzeyde güvence sağlar.
- Son olarak KRY kurumlarda reaktif yönetim tarzından proaktif yönetim tarzına geçilmesine katkıda bulunur. Ayrıca çalışanların performanslarının risk odaklı takibi konusunda gerekli altyapıyı hazırlar.

KRY sisteminin bir diğer önemli faydası da, iç denetçinin risk algılamasını değiştirerek kurumun amaçlarına ulaşmasını engelleyecek risklere odaklanmasını sağlamaktadır. Böylelikle iç denetçinin kuruma değer katma fonksiyonu ön plana çıkmaktadır[129]. Bu durum aynı zamanda iç denetimde planlama ve test aşamalarını etkilemektedir. Sonuç olarak bu süreçler iç denetimin iş yoğunluğunun artmasını da beraberinde getirmektedir[130].

KRY sisteminin beklenen faydaları sağlayabilmesi sistemin etkin çalışıp çalışmadığı ile ilgilidir. Eğer iç denetim birimi KRY sürecinde güvence rolü üstlenmişse, KRY sisteminin etkinliğinin değerlendirilmesi, alınması gereken düzeltme önlemlerinin önerilmesi ve bundan sonraki sürecin takibinde iç denetçi önemli rol oynar.

2.2.2. İç Kontrol Çerçevesi ve Kurumsal Risk Yönetimi Çerçevesi

COSO tarafından yayınlanan iç kontrol çerçevesi ile KRY çerçevesi arasındaki benzerlik, "KRY ile iç kontrol çerçevesinin geçerliliği son mu buldu?" sorusunun uygulamacılar arasında ve akademik platformlarda tartışılmasına neden olmuştur. Ulaşılan sonuç ise iç kontrol çerçevesinin daha çok küçük boyuttaki işletmelere basit düzeyde bir kontrol çerçevesi verdiği ayrıca iç kontrol çerçevesinin KRY için bir temel, ön basamak, olarak benimsenmesi gerektiği şeklindedir[131].

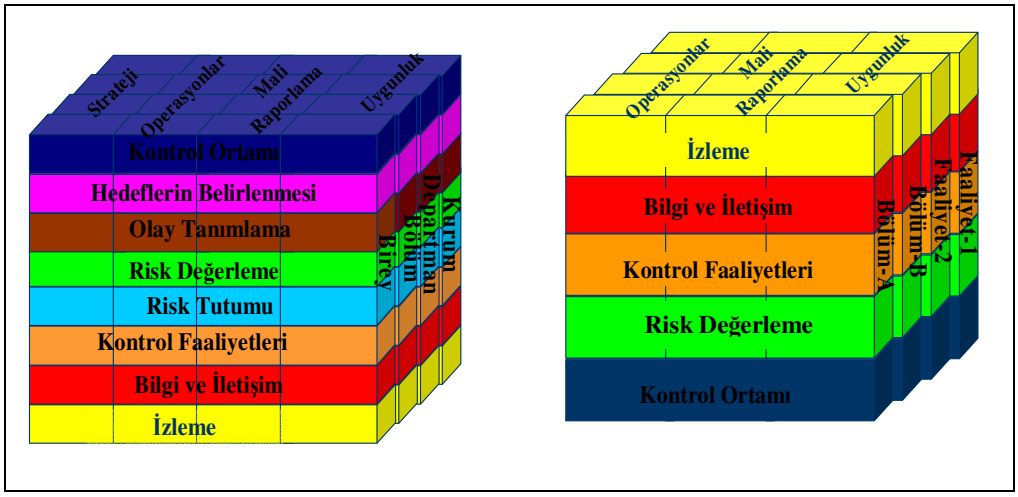
KRY çerçevesi, iç kontrol çerçevesi temelli oluşturulmuştur ve kurum çapında risklerin tanımlanması ve yönetilmesi gerekliliğine vurgu yapılmaktadır[132]. İç kontrol çerçevesi ile KRY çerçevesi arasındaki temel farklılıkların başında ise ilkinin iç kontrol esaslı ikincisinin risk değerleme esaslı tasarlanmış olması gelmektedir. KRY kurumu etkileyebilecek risklerin anlaşılması ve yönetimi için

[129] Walker, Shenkir and Barton, "ERM in Practice", s. 54.
[130] Beasley Mark S., Clune Richard and Hermanson Dana R., "ERM A Status Report", **Internal Auditor,** February 2005, s. 71.
[131] Moeller, **Brink's Modern Internal Auditing,** s. 117.
[132] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 9.

tasarlanmışken iç kontrol çerçevesi ise kurum iç faaliyetlerinin bir gereksinimi olan iç kontrollerin anlaşılması ve yönetimi için tasarlanmıştır. İç kontrol çerçevesi, risk yönetiminin bir bileşeni olmakla birlikte burada ilgi noktası iç kontrol temelli risklerdir öte yandan KRY, işletme temelli risklerin yanısıra organizasyonun genelini ilgilendiren dış çevre kaynaklı riskleri de ilgi alanına eklemiştir[133].

COSO KRY çerçevesi, COSO iç kontrol çerçevesine şekil özellikleri bakımından benzemektedir. KRY küpü iç kontrol küpü gibi, üç boyutlu bir matris şeklinde tasarlanmıştır. Küplerin dikey katmanı amaçlar (hedefler) kategorisinden, yatay katmanı bileşenlerden ve küpün üçüncü boyutu da risklerin ortaya çıktığı yer olan kurum organizasyon yapısından oluşmaktadır.

COSO KRY küpünün dikey katmanı hedeflere ayrılmıştır. KRY'nin hedefleri strateji, operasyonlar, mali raporlama ve uygunluk olarak sıralanırken iç kontrol küpü hedefleri arasında KRY küpünden farklı olarak strateji bulunmamaktadır. Bu durumunda temel nedeni odak noktası, riskler ve kontroller, faklılığından kaynaklanmaktadır.



Şekil 6: COSO KRY Küpü ve İç Kontrol Küpü

Kaynak: Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** USA, 2006, s. 14.

COSO KRY çerçevesinde iç kontrol çerçevesinden farklı olarak ayrıca yatay bileşenlerin sayısı da beş'ten sekize çıkarılmıştır. Yatay bileşenler COSO KRY çerçevesinde kontrol ortamı, hedeflerin belirlenmesi, olay tanımlama, risk

[133] Moeller, **Brink's Modern Internal Auditing,** s. 117.

değerleme, risk tutumu, kontrol faaliyetleri, bilgi ve iletişim ile izleme olarak yer almıştır.

COSO iç kontrol çerçevesinin üçüncü boyutu Bölüm A, Bölüm B, Faaliyet 1 ve Faaliyet 2 olarak sıralanmışken, KRY küpünün üçüncü boyutu bunlardan farklı dört bileşenden oluşmaktadır. Bunlar kurumun genelindeki riskler, departman seviyesindeki riskler, bölüm seviyesindeki riskler ve bireylerden kaynaklanabilecek risklerdir.

KRY çerçevesi iç kontrol çerçevesi gibi üç boyutu da birbirine geçişli tasarlanmış olup bileşenleri amaçlardan ve her ikisini de kurum seviyesinde yürütülen faaliyetlerden ayırmanın olanağı yoktur. KRY küpü bir bütün olarak ele alınmalıdır.

2.2.3. Kurumsal Risk Yönetimi Hedefleri

Misyon ve vizyonları çerçevesinde stratejik hedeflerini belirleyen kurumlar bunları sıraladıktan sonra ilgili kurum çalışanları ile paylaşırlar. Hedeflerin belirlenmesi işlemi kurum geneli için olabileceği gibi departman bazında da yapılabilir. KRY çerçevesi, kurum hedeflerinin başarılmasına odaklanmıştır ve bu hedefler dört kategoriye ayrılmıştır[134]:

- Strateji
- Operasyonlar (Faaliyetler)
- Raporlama
- Uygunluk

Stratejik amaçlar, yüksek düzey hedeflerle ilgilidir ve firma misyonunu desteklemelerine göre sıralanırlar. Faaliyetlere ilişkin amaçlar ise kurum kaynaklarının etkin ve verimli kullanımı ile ilgilidir[135].

Diğer yandan KRY'den raporlamanın güvenilirliğine ve yürürlükteki kanun ve düzenlemelere uyuma ilişkin makul derecede güvence sağlaması beklenir. Bu

[134] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management – Integrated Framework (Executive Summary),** s. 3.
[135] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 11.

kategorideki amaçlara ulaşılması kontrollere ve bunlarla ilgili faaliyetlerin nasıl yürütüldüğüne bağlıdır[136].

Sonuç olarak, stratejik amaçlar -pazar payında belirli bir seviyeye ulaşmak- ve faaliyetlere ilişkin amaçlar -yeni ürünün pazara başarılı bir şekilde sunulması gibi- genellikle kurum kontrolleri dışındadır. KRY, dış çevre kaynaklı olaylar veya durumlarla ilgili kötü sonuçları engelleyemez. Fakat yönetimin daha iyi kararlar alma olasılığını artırabilir[137]. Raporlama ve uygunluk kurum yapısıyla ilgilidir ve dış çevre kaynaklı olaylara göre kontrolü ve yönetimi daha çok mümkündür.

2.2.4. Kurumsal Risk Yönetimi Bileşenleri

KRY birbiri ile ilişkili sekiz bileşenden oluşmaktadır. Bunlar sırasıyla kontrol ortamı, hedef belirleme, olay tanımlama (risk tanımlama), risk değerleme, risk tutumu, kontrol faaliyetleri, bilgi ve iletişim ve son olarak da izlemedir. Son iki bileşen, bilgi ve iletişim ile izleme, bütün olarak KRY küpünün üzerinde etkinliği olan diğer yatay dikey ve katmanlar ile üçüncü boyutta yer alan bileşenleri de kapsayan bir süreçtir.

Nihai olarak her kurumun KRY algılaması ve uygulaması farklılık gösterebilmektedir. Bu farklılığın nedeni faaliyette bulunulan sektörler olabileceği gibi kurum büyüklüğü, kültürü ve yönetim felsefesi temelli de olabilir. Bu nedenle kurumlarda uygulanan kontrol yapıları ve KRY çerçeveleri farklı olabilir. Bu da genel olarak KRY bileşenlerinin uygulamadaki ağırlıklarını ve dikkate alınma düzeylerini etkileyecektir.

2.2.4.1. Kontrol Ortamı

Diğer KRY bileşenleri için temel oluşturan ve KRY'nin ilk aşaması olan kurum kontrol ortamı, kurum geçmişi ve kültürü temelli bir yapıdır[138]. Kontrol ortamının anlaşılması kurumun faaliyetlerini gerçekleştirirken karşılaşabileceği risklerin anlaşılabilmesi için temel şarttır[139]. Bu nedenle kontrol ortamı hakkında

[136] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 11.
[137] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 11.
[138] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 19.
[139] Funston, **a.g.e.,** s. 1.

yeterli bilgiye sahip olmak KRY sisteminin kurulması ve KRY bileşenlerinin etkinlikleri açısından önemlidir.

Kontrol ortamını etkileyen temel faktörler risk yönetim felsefesi, etik değerler, risk kültürü, risk tutumu, yönetim kurulu, yönetim felsefesi ve yönetim faaliyet stili, sorumluluk ve görev dağılımları son olarak da insan kaynakları politikaları ve uygulamaları şeklinde sıralanabilir[140].

Kontrol ortamının öne çıkan önemli bileşenleri risk kültürü ve buna bağlı olarak risk tutumudur. Kurum faaliyetlerinde aynı koşullarda aynı kararların alınması açısından risk kültürünün önemli bir rolü vardır ve risk kültürü ile tutumunun oluşturulması bir yönetim faaliyetidir[141].

Kontrol ortamı kurum genelinde yapılan denetimlerde dikkate alındığı gibi departman veya bir alana yönelik yapılan denetimler içinde temel bir bileşendir. Genel olarak kontrol ortamının anlaşılması aşağıdaki faaliyetlerden meydana gelir[142]:

- Süreç tanımlaması,
- Anahtar girdilerin belirlenmesi; dış kaynaklardan gelen belgeler, diğer süreçlerin veya alt süreçlerin çıktıları, dış kaynaklardan bilgiler ve iç sistemlerden veriler,
- Anahtar adımların belirlenmesi; kontrol ve izleme görevleri, tamamlanmış faaliyetlerin analizi, alınan kararlar, sistem güncelleştirmeleri, görevleri gerçekleştiren anahtar personel ve görevler için gerekli zaman,
- Anahtar çıktıların belirlenmesi; kurum dışına gönderilen belgeler, iç kullanıcılar için raporlar, diğer süreçler için veriler, bilgisayarda depolanan veriler ve fiziksel olarak belge depolaması,
- Anahtar kontrollerin belirlenmesi,
- Yönetilebilir risklerin belirlenmesi.

[140] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 19.
[141] Griffiths Phil, **a.g.e.,** s. 19.
[142] Sobel, **a.g.e,** s. 8.09.

Kontrol ortamının anlaşılmasına yardımcı olacak belgeler risk politikaları ve risk stratejilerine ilişkin belgeler, finansal tablolar ile ekleri, yıllık işletme planı ve stratejik planlar olarak sıralanabilir[143].

Sarbanes-Oxley yasasının 4. bölüm 404 numaralı kısmında finansal raporlama ve risklerle ilgili kurum kontrol ortamı düzenlemelerine yer verilmiştir[144]. Burada yer alan düzenlemeler COSO İç Kontrol ve KRY Çerçeveleri ile paraleldir. Yasanın bu kısmında COSO İç Kontrol Çerçevesinde yer alan bileşenlere atıflar vardır.

2.2.4.2. Hedeflerin Belirlenmesi

Her kurum iç ve dış kaynaklı pek çok riskle karşılaşmaktadır. Olay tanımlamalarının, risk değerlemelerinin ve risk tutumlarının etkin belirlenebilmesi farklı seviyelerdeki kurum hedeflerinin tam ve doğru olarak belirlenebilmesine bağlıdır. Hedefler stratejik açıdan, faaliyet temelli, raporlamaya ilişkin ve uyum-uygunluk temelli olarak belirlenebilir[145].

Hedeflerin belirlenmesi sürecinde, kurum stratejileri, risk alma istekliliği sınırları, risk toleransı ve bütün bunların kurum vizyon ve misyonu ile olan ilişkileri dikkate alınmalıdır. Aksi halde belirlenen hedefler birbirleriyle çelişebilecek veya ulaşılması imkânsız olabilecektir[146].

Kurumun merkezden ayrı birimlerinde, departman seviyesinde ve ikincil alanlar içinde hedefler kurum genel hedefleriyle bütünleşecek şekilde CEO (Genel Müdür) rehberliğinde ilgili birim yöneticileri tarafından belirlenir[147]. Bir kurumun hedefleri ve buna bağlı olarak belirlenmiş olan stratejilerinin bulunması, o kurumun değer yaratma ve risk yönetimi uygulamaları için sağlam bir zemin oluşturduğunu gösterir[148].

---

[143] Norman Buckley, **It's a Risky Business: a Practical Guide to Risk Based Auditing,** The Chartered Institute of Public Finance and Accountancy (CIPFA), UK, 2005, s. 9.
[144] USA Congress, Sarbanes-Oxley Act Of 2002, Chapter 4, Section 404.
[145] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 19.
[146] Schanfield Arnold and Miller Michael, "A Sustainable Approach to ERM", **Internal Auditor,** April 2005, s. 1.
[147] Matyjewicz and D'arcangelo., "Beyond Sarbanes-Oxley", **Internal Auditor,** November/December 2004, s. 69.
[148] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 23.

KRY açısından kurum vizyonu, misyonu ve stratejisi çerçevesinde belirlenen hedeflerin risk alma istekliliği paralelinde sıralamasını üst yönetim, genellikle CEO, yapar. Yanlış sıralama amaçların başarılması için risklerin kabul edilmediği veya yersiz-gereksiz risklerin kabul edildiği anlamına gelmektedir[149].

Hedeflerin belirlenmesi sürecine yön veren ve risk-hedef ilişkisini daha anlaşılır kılan anahtar dokümanlar; yönetim kurulu ve denetim komitesi çalışma kâğıtları ve raporları, gerçekleştirilen eğitim faaliyetleri ve bunlara ilişkin belgeler, kontrol hatları ve iş tanımlarına ilişkin belgeler olarak ifade edilebilir[150].

KRY temelli çalışan bir denetim sisteminde iç denetim birimi, işletme ve departman düzeyinde belirlenen amaçlar ve hedefler çerçevesinde denetim süreçlerini planlar. Denetimin planlama sürecinin amacı, işletme hedeflerinin etkili bir şekilde belirlenip belirlenmediğini ve bu amaçların kurum genelinde duyurulup duyurulmadığını tespit etmektir. Bu değerlemeler sonucunda iç denetçi KRY sürecinin yardımıyla denetim evreni için gerekli bilgilere ulaşır[151].

2.2.4.3. Olay Tanımlama

KRY bileşenlerinden üçüncüsü olan olay tanımlama, risk tanımlama olarak da ifade edilebilmektedir. Bu aşamada, kurum kontrol ortamı ve belirlenen hedefler çerçevesinde kurumun hedeflerine ulaşmasının önündeki engeller diğer bir ifadeyle riskler tanımlanır. Risk tanımlamalarına, kurumun hedeflerine ulaşmasını etkileyebilecek her türlü iç ve dış olay dahil edilir[152].

Olay (risk) tanımlama ve bunu izleyen aşama olan risk değerleme sürecine kurum risk alma istekliliği yön verir. Kurum yönetim kurulu ve üst düzey yöneticiler tarafından belirlenecek olan risk alma istekliliği kurum risk kültürü ile yani kurumun risklerden kaçan bir yapıda mı yoksa risk alan bir yapıda mı olduğuyla ilişkilidir[153].

Hiyerarşik yapının baskın olduğu, stratejilerin çok sık değişmediği ve hataların genellikle kişiselleştirildiği kurum kültürünün bir ürünü olan risklerden

[149] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 35.
[150] Buckley, **a.g.e.,** s. 11.
[151] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 5.
[152] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 38.
[153] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 12.

kaçan yapının tersine risklere açık bir yapı ise stratejilerin sıklıkla değiştiği, kurum odak noktasının dış kaynaklı olaylar olduğu ve hataların kabul edilebilir olarak benimsendiği bir kurum kültürünü özetler[154].

Bu açıdan kurum risk alma istekliliğinin ve risk tanımlamalarının sağlıklı olarak yapılabilmesi, kurum risk kültürünün hangi tür bir yapıda olduğu ile ilişkilidir.

Kurum risk alma istekliliğinin belirlenmesi bir üst yönetim fonksiyonudur. İç denetçi bu rolü üstlenmemelidir. Bununla beraber iç denetçi bu aşamada üst yönetime risk alma istekliliği seviyelerinin belirlenmesinde, risklerin ölçülmesinde ve etkili bir şekilde kurum politika, süreç ve uygulamalarına dönüştürülmesinde danışmanlık sağlayabilir veya güvence hizmetini üstlenebilir. Bu süreçte iç denetçi, üst yönetime kurum genelinde belirlenen risk alma istekliliği sınırlarına uygun hareket edildiğine ilişkin güvence verir [155]. İç denetçinin kurum genelinde hemen hemen her alana ulaşabilmesi risk tanımlamalarında bir avantaj olarak görülebilir. Bu sayede kurum genelinde riskler kolaylıkla tanımlanabilir[156].

A. Risk Tanımlamaları İçin Gerekli Veriler

Risk tanımlamalarında kullanılacak veriler kurum iç ortamından ve daha önceden belirlenen kurum hedeflerinden elde edilir. Risk tanımlama süreci sonucunda ise risk kaynaklarına, riske neden olabilecek potansiyel olaylara, risk belirtilerine ve KRY'nin bundan sonraki aşamaları için temel verilere ulaşılır[157].

Risk tanımlama sürecine yön veren temel belgeler işletme stratejik planı ve hedefleri[158], kontrol listeleri, kayıtlara ve deneyimlere bağlı çıkarımlar, akış diyagramları, sistem analizleri, senaryo analizleri, sistem mühendislik teknikleri[159], yöneticiler ve risk çalıştayı ajandası için hazırlanmış olan risk değerleme rehberi ve son olarak da riskler hakkındaki sektör rehberleridir[160].

---

[154] Griffiths Phil, **Risk-Based Auditing,** Gower Publishing, USA, 2005, s. 20.
[155] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 12.
[156] Hespenheide Eric, Pundmann Sandy and Corcoran Michael, "Risk Intelligence: Internal Auditing In A World Of Risk" **Internal Auditing,** Jul/Aug 2007, s. 6.
[157] Merna Tony and Al-Thani Faisal F., **Corporate Risk Management,** John Wiley & Sons, USA, 2005, s. 39.
[158] Institute of Management Accountants, Statements of Management Accounting, **Enterprise Risk Management: Frameworks, Elements, and Integration,** s. 26.
[159] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 37.
[160] Buckley, **a.g.e.,** s. 13.

Kurum stratejik planı ile riskler arasında yüksek düzeyde bir ilişki vardır. Eğer stratejilerin belirlenmesi aşamasında riskler dikkate alınmazsa kurum stratejileri etkinliklerini kaybedebilir tam tersi durumda ise riskler belirlenirken stratejiler ihmal edilirse kurum açısından çok önemli ve belki de yüksek riskli alanlar gözardı edilmiş olur[161].

B. Risklerin Kaynakları ve Fırsatlar

Risk tanımlama sürecinin önemli bir aşaması da risklere neden olan olayların işletme içi faktörlerden mi yoksa işletme dışı faktörlerden mi kaynaklandığının belirlenmesidir. Risklerin kaynaklarının anlaşılması risklerin etkin ve etkili yönetimi için ilk adımdır. Kaynağı belirlenemeyen riskin yönetim süreci oldukça zordur[162]. Kurum içi nedenlerden kaynaklanabilecek risklerin yönetimi dış kaynaklardan doğabilecek risklere göre daha kolaydır. Bununla beraber risklere kurum yönetimi tarafından uygulanan stratejiler neden olur ve bunların iyi anlaşılması risk tanımlamaları açısından çok önemlidir[163].

Risklere neden olabilecek dış olaylar ekonomik, doğal çevre, politik ve sosyal yapıdan kaynaklanabileceği gibi teknolojideki değişmelerden de kaynaklanabilirler. Kurum içi risk kaynakları ise bina, ekipman, alt yapı, personel, üretim ve hizmet süreçleri olarak sıralanabilir[164].

Risk tanımlama sürecinde, riskler ve fırsatlar arasındaki ayrıma dikkat edilmelidir. Olayların hem negatif-olumsuz etkileri hem de pozitif-olumlu etkileri olabilir. Riskler bir olayın negatif yönünü yansıtırken fırsatlar ise olayın pozitif yönünü yansıtırlar[165].

Risk tanımlama ve bunu izleyen aşama olan risk değerleme süreci risk ve fırsatlar arasındaki optimum dengeyi bulmalı, ayrıca risk-fırsat ilişkisini

---

[161] Institute of Management Accountants, **a.g.e.,** s. 26.
[162] Sobel, **a.g.e,** s. 2.09.
[163] The Institute of Chartered Accountants England & Wales, **Risk Management and the value added by internal audit**, The Institute of Chartered Accountants England & Wales, UK, 2000, s. 4.
[164] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 39.
[165] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management – Integrated Framework (Executive Summary),** s. 4.

maliyet-fayda boyutunda ele alarak kurum risk alma istekliliği sınırları içinde hareket etmelidir[166].

C. Risk Tanımlamalarında Kullanılan Yöntemler

Karakteristikleri analiz edilen risklerin tanımlanmasında ve değerlendirilmesinde kullanılabilecek çeşitli araçlar mevcuttur. Bunlar çalıştay, görüşme, senaryo planlaması, anket, beyin fırtınası, sektör karşılaştırmaları, geçmiş hataların analizi, tarihsel veriler temelli tanımlama, performans gözden geçirmeleri ve çalışan-müşteri geri beslemeleri olarak sıralanabilir[167].

Risklerin tanımlanması ve değerlendirilmesi sürecinde en yaygın kullanılan yöntem kontrol-risk öz değerlendirme programı çerçevesinde risk çalıştayları düzenlemektir. Farklı sorumluluk alanlarından çalışanları, üst düzey yönetici ile tezgah görevlisi gibi, bir araya getiren risk çalıştayı risklerin etkilerinin farklı görüş açılarından değerlendirilmesini sağlar. KRY ile merkezileştirilen risk yönetiminin ve risk değerlemelerinin faaliyet temeli yapılması ve kurum çapında değerlendirilmesi ihtiyacı risk çalıştayları ile mümkün olur[168].

Risk çalıştayları, tanımlanan riskler ve risk listeleri hakkında fikir birliğine ulaşmayı, daha önceden seçilen bilgisayar yazılımı desteğiyle risklerin değerlendirilmesini içeren oylama faaliyetinin gerçekleştirilmesini ve oylama sonucuna göre risklerin sıralanmasını, eylem planlamasını kapsayan risk tutumlarının belirlenmesini, anlık raporlama ve eğitim faaliyetlerini içerir[169]. Bilgisayar destekli olmayan çalıştaylarda ise katılımcılara dağıtılan temel işletme süreçleri arasından riskleri işletmeye/finansal performansa etkisi ve süreç/kontrol zayıflığı olasılığına göre değerlendirmeleri ve yine katılımcılara dağıtılan boş risk haritasına, seçtikleri riskleri yerleştirmeleri istenmektedir.

Risk tanımlama ve değerlendirmelerini içeren çalıştay için öncelikle risk kavramı, risk çerçevesi, risk kaynakları ile risklerin olasılık ve etki tanımlarının yer

---

[166] Merna and Al-Thani, **a.g.e.,** s. 41.
[167] Griffiths Phil, **a.g.e.,** s. 23., Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 21., Institute of Risk Management (UK), **A Risk Management Standard,** UK, 2002, s. 16., El-Dine Dani Saad, **Control Self Assessment Concepts and Applications,** Thomson, Canada, 2005, s. 236., Collier Paul M., Berry Anthony J. and Burke Gary T., **Risk and Management Accounting,** CIMA Publishing, UK, 2007, s. 11.
[168] Booker Fay M., "An ERM Framework: Developing Effective Risk Management Strategies to Protect Your Organization", **White Paper,** August 2003, s. 2.
[169] Walker, Shenkir and Barton, **Enterprise Risk Management: Pulling it all Together,** s. 22.

aldığı bir rehber hazırlanmalıdır[170]. Çalıştaylarda, katılımcıların risk tanımlarında ve listelenen risklerin yeterliliği konusunda hemfikir olmaları temel düzeyde bir yanlışlığa neden olmamak için önemlidir[171].

Risk çalıştayları esnasında katılımcıların etkileşim halinde bulunması, yeni fikirlerin ve gizlenmiş ayrıntıların ortaya çıkarılmasına yardımcı olur[172]. Risk çalıştayları özellikle yeni projelere, yeni iş alanlarına veya kuruma zarar gelmesi muhtemel alanlara uygulandığı zaman kuruma artı değer kazandırır[173].

Çalıştayların yanısıra risk tanımlama ve risk değerleme sürecinde kullanılan bir diğer araç da görüşme yöntemidir. Risklerin tanımlanması sürecinde kullanılan ve temel amacı kurum hedefleri arasında gizli olan riskleri ortaya çıkarmak olan bire bir görüşme yöntemi, grup toplantılarından daha kolay düzenlenir ve ayrıca çalışanlar geniş katılımlı toplantılara göre daha fazla fikirlerini açıklamaya isteklidirler[174]. Bunların yanısıra görüşme yönteminde katılımcılar arasında iletişimin olmaması etkileşimi ve risklerle ilgili olası tartışmaları engellemekte ve böylece risk çerçevesi daha kolay çıkarılabilmektedir[175]. Öte yandan bu yöntem tartışma ortamının sağlayacağı faydaları ortadan kaldırmaktadır.

İfade edilen avantajların yanısıra geniş yelpazede risklerin belirlenmesi, sınıflandırma işlemini zorlaştırır. Ayrıca risklerin olasılık ve etkilerinin kesinleştirilmesi için görüşmenin ardından geniş katılımlı risk çalıştayı yapılması zorunludur[176].

Beyin fırtınası yöntemi de risklerin tanımlanması sürecinde sıklıkla kullanılmaktadır. Kurum yönetiminde görevli ve bu özellikleri dolayısıyla da kurumu en iyi tanıyan çalışanların tartışmaları ve bu sürecin sonunda belirli riskler üzerinde uzlaşmaları gerçekçi bir şekilde risklerin belirlenmesine ve tanımlanmasına imkân verir[177].

---

[170] Wade Keith and Wynne Andy (Editors), **Control Self Assessment,** John Wiley & Sons, USA, 1999, Chapter 8, s. 137.
[171] Walker, Shenkir and Barton, **Enterprise Risk Management: Pulling it all Together,** s. 130.
[172] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 21.
[173] Pickett and Pickett, **Auditing For Managers The Ultimate Risk Management Tool,** s. 95.
[174] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 21.
[175] Flexner William A., "Risk Self Assessment: Increasing Speed, Quality and Focus in the Audit Planning Process", **Option Technologies,** Summer 1996, s. 1.
[176] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 21.
[177] Sobel, **a.g.e,** s. 5.08.

Risklerin tanımlanması aşamasında kullanılacak bir diğer yöntem de kurum geçmişine ait verilerin incelenmesidir. İncelenecek veriler muhasebe kökenli olabileceği gibi geçmiş dönem denetim çalışma kâğıtları, müşteri şikâyetleri, iş akış şemaları ve faaliyetlerin yürütülmesi sırasında uyulması geren yönetmelikler de dahil olmak üzere geniş kapsamlı olarak düşünülebilir[178].

KRY'de kullanılan bu araçlar hakkında ayrıntılı incelemeler ve değerlendirmelere bu bölümün üçüncü kısmı "Kurumsal Risk Yönetimi Araçları" başlığı altında yer verilecektir.

D. Risklerin Sınıflandırılması

Risk tanımlama süreci tanımlanan risklerin sınıflandırılması ile son bulur. Farklı bilim dalları ve farklı sektörler için pek çok risk sınıflandırması yapılabilmekle beraber, sistematik ve sistematik olmayan risk gibi[179], burada dikkate alınan sınıflandırma KRY sistemini uygulamada kullananlar tarafından en çok tercih edilen sınıflandırmadır[180]:

1. Stratejik riskler: Orta ve uzun vadede kurum hedeflerini etkileyebilecek olan risklerdir. Bunlar da kendi içinde politik, ekonomik, sosyal ve müşteri kaynaklı olarak çeşitlendirilebilir.
2. Operasyonel riskler: Günlük faaliyetlerin yürütülmesi esnasında yönetim ve çalışanların karşılaştığı risklerdir. Bu riskler rekabete dayalı, fiziksel ve sözleşmeye dayalı nedenlerle ortaya çıkabilirler.
3. Finansal riskler: Finansal planlama, bütçe kontrolü, likidite sıkışıklığı veya yetersiz izleme ve raporlama temelli risklerdir.
4. İtibar riski: Kurum ismine zarar verecek her türlü olayı içerir.
5. Bilgi teknolojileri riski: Teknolojik eksikliklerden kaynaklanabileceği gibi fiziksel bilişim araçları temelli de olabilir.
6. Düzenleme riski: Ulusal veya uluslararası düzenleme otoritelerinden, çevresel nedenlerden (çevre kirliliği, arazi kullanımı gibi) veya kanunlardan kaynaklanabilecek risklerdir.

[178] El-Dine Dani Saad, **a.g.e.,** s. 236.
[179] Rodoplu Gültekin, **Para ve Sermaye Piyasaları,** Isparta, Tuğra Ofset, 2002, s. 362.
[180] Griffiths Phil, **a.g.e.,** ss. 22-23.

7. Birey temelli riskler: Profesyonel insan kaynağı yetersizliklerinden kaynaklanabileceği gibi kilit personelin kaybından da kaynaklanabilir.

İç denetçi, kurum risk yönetimi olgunluk seviyesi ve organizasyon itibariyle kendine biçilen sınırlar dahilinde risk tanımlama aşamasında aktif görev alabileceği gibi sürecin etkinliğinin denetiminden de sorumlu tutulabilir. Eğer risk tanımlama aşaması risk yönetim birimi tarafından üstlenilmişse iç denetçi, güvence fonksiyonunun gereklerini yerine getirir.

Bu aşamada, güvence verme fonksiyonu kapsamında iç denetçi öncelikle risk evrenini inceler ve önemli riskleri değerlendirir. İç denetçi, risk tanımlamaları, sınıflandırmaları ve diğer özellikleri kurum genelinde uygulamada bütünlük olması açısından değerlendirir. Bu çerçevede denetçi, kurum hedefleri ve stratejiler ile riskler arasındaki ilişkiyi de dikkatle inceler. Eğer varsa uygunsuz ve eksik riskler denetçi tarafından üst yönetime rapor edilir[181].

2.2.4.4. Risk Değerleme

COSO tarafından yayınlanan iç kontrol çerçevesinin bir bileşeni olan risk değerleme aynı zamanda iç denetim standartlarında denetimin planlanması aşamasında önerilen bir çalışmadır ve KRY bileşenleri içinde de anahtar bir rolü bulunmaktadır.

KRY bileşenlerinden kontrol ortamı, hedef belirleme ve olay tanımlama aşamaları diğer aşamalar için bir bilgi toplama ve çerçevenin çizilmesi olarak görülebilirse de, bundan sonraki aşamalar -risk değerleme, risk tutumu, bilgi ve iletişim ve izleme- risklere karşı faaliyet alanıdır ve bu faaliyetlere risk değerleme sürecinin çıktıları yön verir.

Risk değerlemesi, kurum hedeflerine ulaşmayı engelleyecek daha önceden tanımlanan ve sınıflandırılan risklerin ölçülmesi ve sıralanması aşamalarını içerir. Risk değerlemesi sonucunda, denetçi denetim programındaki testleri önemli kontrol noktalarına uygulayabilir[182].

---

[181] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 7.
[182] Selim Georges and McNamee David, "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change", **International Journal of Auditing,** Vol: 3, 1999, s. 168.

Riskler, değerlemede kullanılacak olan nitel (kalitatif) veya nicel (kantitatif) yöntemlerden biri veya karması yardımıyla olasılık ve etkileri açısından ölçülürler. Ardından ölçülen riskler risk matrisi-haritası yardımıyla sıralanırlar.

A. Nitel – Nicel Analiz

Temel risk yönetimi süreci olan risk değerlemeleri ve diğer süreçler resmi-gayri resmi, nitel-nicel veya ilgili iş birimi-kurum geneli merkezli olarak gerçekleştirilebilir[183].

Risk karakteristiklerinin belirlenmesi adımını değerlemede kullanılacak yöntemin seçimi izler. Risk değerlemesi yöntemleri, nitel ve nicel tekniklerin bütünleştirilmiş şekli olmalıdır. Nitel değerlendirme teknikleri, potansiyel olasılık ve etkinin düşük olduğu veya sayısal verinin ve nicel değerlendirme uzmanının bulunmadığı koşullarda kullanılmaktadır[184].

Nitel analiz, olayların potansiyel etkilerinin derecesinin ve bunların ortaya çıkma olasılıklarının, analizi gerçekleştirenlerin bireysel yargıları ile ifade edilmesidir[185]. Başlıca nitel değerleme teknikleri; beyin fırtınası, Delphi analizi tekniği, görüşme tekniği, kontrol listeleri, risk kayıtlaması, risk haritalaması ve son olarak da olasılık-etki tablolarıdır[186].

Nitel değerleme tekniklerini kurum risk kültürü-tutumu yönlendirmektedir. Eğer kurum risklere karşı isteksiz bir yapıdaysa geleceğin belirsizliğini mümkün oldukça azaltmak isteyecek, bir başka ifadeyle riskli faaliyetlerden kaçınmaya yönelik bir değerlendirme sonucuna ulaşılacaktır. Öte yandan kurum, risklere karşı açık yani risk arayan bir yapıda ise riskin olumsuz etkileri karşısında endişelenmeyen ve fırsatlar konusunda iyimser tavır sergileyen bir yapıda olacaktır. Sonuç olarak risk değerlemeleri riskli faaliyetleri onaylayacaktır[187].

Olasılık dağılımlarının ve etkilerin rakamsal olarak belirlenmesine yönelik çalışmaların yürütüldüğü yönteme nicel değerlendirme yöntemi denir. Ancak bu yöntem ulaşılabilir uygun veriler ve yeterli sayıda uzman personel olduğu

[183] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2110-1.
[184] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 143.
[185] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 40.
[186] Merna and Al-Thani, **a.g.e.,** ss. 56-63.
[187] Hillson and Murray-Webster, **a.g.e.,** s. 26.

durumlarda kullanılabilir[188]. Nicel analiz sonuçlarının kalitesi kullanılan verinin doğruluğu ve bütünlüğü ile kullanılan modelin geçerliliğine bağlıdır[189].

Olasılık ve etkilerin tahmininde kullanılan kurum geçmiş olaylarının gözlemlenmesi sonucu elde edilen veriler, subjektif tahminlere göre daha objektiftir. Kurum geçmişinden derlenecek tarihi veriler dış kaynaklardan elde edilecek verilere göre daha iyi sonuçlar sağlar. Bununla beraber iç kaynaklardan derlenen veriler başlangıç aşamasında yeterli olmakla birlikte dış kaynak kökenli veriler kontrol noktası olması açısından önemlidir[190].

Nicel değerlendirme teknikleri genellikle bilgisayar temelli tekniklerdir. Bu tekniklerin başlıcaları karar ağacı tekniği, Monte Carlo simülasyon programı, duyarlılık analizleri ve olasılık-etki grid analizleridir[191]. Nitel ve nicel tekniklerin kullanımına imkân veren diğer yönetim araçları risk tanımlama ve değerlendirme aşamalarında da kullanılan kontrol-risk öz değerlendirme çatısı altında görüşme tekniği ve çalıştaylardır[192].

Literatürde nitel değerleme teknikleriyle elde edilen verilerin nicel değerleme teknikleriyle elde edilen verilerden daha kullanışlı olduğuna ve özellikle KRY sisteminin kurulması ve başlangıç aşamasında nitel değerleme yöntemlerinin tercih edilmesi gerektiği yönünde görüş birliği vardır[193].

Risklerin değerlendirilmesi sürecinde dikkate alınması gereken bir diğer önemli konu da risklerin içsel veya kalıntı risk sınıflandırmasından hangisine dahil olduklarıdır. İçsel riskler, herhangi bir kontrol mekanizmasının bulunmadığı durumlarda işlem süreçlerinin doğasında varolan risklerdir. Artık risk olarak da ifade edilebilen kalıntı riskler ise alınan kontrol önlemlerine rağmen mevcut olan risklerdir[194].

---

[188] Merna and Al-Thani, **a.g.e.,** s. 56.
[189] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 41.
[190] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 49.
[191] Merna and Al-Thani, **a.g.e.,** s. 56.
[192] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 50.
[193] Merna and Al-Thani, **a.g.e.,** s. 56.
[194] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 18.

Risk değerleme faaliyeti öncelikle içsel risklere uygulanır ardından kalıntı riskler ölçülür[195]. Alınan iç kontrol önlemlerinden önce ortaya çıkacak olan risklerin önem ve olasılıkları değerlendirilerek içsel riskler ölçülür. Alınan iç kontrol önlemlerinden sonra ortaya çıkacak olan risklerin önem ve olasılıkları değerlendirilerek kalıntı riskler ölçülür[196].

Risk değerlemeleri makro ve mikro düzeyde gerçekleştirilebilir. Makro risk değerlemesi; denetim önceliklerinin belirlenmesi, denetim kaynaklarının en riskli faaliyetlerden başlatılmasını hedefler[197] ve denetim hizmeti alması gereken doğru alanların denetlendiğine ilişkin güvence sağlar[198].

Mikro risk değerlemesi ise denetlenen faaliyete ilişkin risklerin tanımlanması, mevcut iç kontrollerin değerlendirilmesi, risklerin giderilmesine yönelik iç kontrol uygulamalarının geliştirilmesini kapsar[199]. Mikro risk değerlemesi de temel olarak iç denetim birimi tarafından doğru alanların denetlendiğine ilişkin güvence vermeye yöneliktir[200].

B. Olasılık – Etki Analizi

Risk değerlemesinde kullanılacak faktörler -olasılık, etki, üçlü veya beşli ölçek, nitel veya nicel değerleme yöntemlerinin kullanımı- risk değerlemesinin yapılması amacına, zamanın elverişliliğine, uzman personelin varlığına, katılımcıların bilgi seviyesine ve beklentilerine ve son olarak ulaşılması istenen sonuçlara bağlıdır. Kurum bu faktörleri dikkate alarak risk değerleme faaliyetini gerçekleştirir[201].

Riskler genellikle ortaya çıkma olasılıklarına ve ortaya çıktıklarında organizasyona etkilerine göre analiz edilirler. Risklere ait olasılık ve etkinin bileşimi sonucuna göre risk sıralaması yapılır[202]. Risk = f (Etki, Olasılık) olarak formüle edilebilir.

---

[195] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 48.
[196] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 18.
[197] Özbek, **a.g.e.**
[198] Hubbard Larry D., "Assessing Risk", **Internal Auditor,** August 2002, s. 2.
[199] Özbek, **a.g.e.**
[200] Hubbard, **a.g.e.,** s. 2.
[201] Sobel, **a.g.e,** s. 6.02.
[202] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 13.

Etki, kurum hedeflerinin başarılamaması ve kurum stratejilerinin başarılı bir şekilde yürütülememesi durumunda doğabilecek zarardır. Etki, kurum itibarının zarar görmesi veya başka faktörlerle de ilgili olabilir. Genellikle finansal veya stratejik etki ölçekleri kullanılmakla birlikte risk değerlemesinin amacına bağlı olarak itibar ve sağlık-güvenlik ölçekleri de kullanılabilir. İzleyen tabloda finansal, itibar ve sağlık-güvenlik beşli ölçekleri karşılaştırmalı olarak ele alınmıştır[203].

Tablo 4: Karşılaştırmalı Beşli Etki Ölçeği

	Finansal	İtibar	Sağlık-Güvenlik
1	Kazanç etkisi yok	İtibara etkisi yok	Sağlık-güvenlik etkisi yok
3	Bir haftalık kazanç	Kurum içi itibarı etkiler	Küçük yaralanmalar (bir kişi için)
5	Bir aylık kazanç	Yöresel itibarı etkiler	Büyük yaralanmalar (bir kişi için)
7	Çeyrek dönemlik kazanç	Bölgesel itibarı etkiler	Büyük yaralanmalar (çok sayıda kişi için)
9	Bir yıllık kazanç	Ulusal-Uluslararası alanda itibarı etkiler	Çalışanlardan veya halktan ölüm

Kaynak: Paul Sobel, **Auditor's Risk Management Guide Integrating Auditing and ERM,** s. 6.05.

Örneğin etki 1 olarak ölçülmüşse; bu, finansal açıdan bir zararın olmadığı, itibara bir etkisinin bulunmadığı ve sağlık-güvenlik etkisinin bulunmadığı anlamına gelmektedir. Bu durumun tam tersi olan seviye, etkinin 9 ölçülmesi halinde finansal kayıp bir yıllık kazanca eşittir, itibari açıdan kayıp ise ulusal-uluslararası itibarın etkilenmesi anlamına gelir. Sağlık güvenlik açısından ise çalışanlar veya halk arasında ölümlere yol açılması anlamına gelmektedir.

Olasılık ise genellikle zaman ile ilgilidir ve olayın meydana gelme sıklığını gösterir[204]. Risk olasılıkları en basit şekliyle düşük, orta ve yüksek olarak sınıflandırılırken risk etkisi de aynı şekilde en basit biçimiyle küçük, orta ve ağır olarak sınıflandırılabilir[205]. Bu ölçeklendirme risklerin ne kadar hassas değerlendirdiğiyle ilgilidir. Olasılık ve etkilerin üçlü ölçekle gösterimi ölçek sınırlarının net olmaması nedeniyle subjektiflik içermektedir. Ölçek derecelendirmesi sınırlarının objektif olmaması ve bireyler arasında farklılık gösterebilmesi değerlendirme faaliyetine, sonuçta risk matrisine karşı bir güvensizliğe neden

[203] Sobel, **a.g.e,** s. 6.03-05.
[204] Griffiths Phil, **a.g.e.,** s. 60.
[205] HM Treasury, The Orange Book, Management of Risk-Principles and Concepts, UK, 2004, s. 19.

olabilir[206]. Bu durumun önüne geçmek için de genellikle beşli ölçek tercih edilmektedir.

Risklerin etki boyutunun değerlendirilmesinde kullanılacak beşli ölçek; önemlilik yok, küçük seviyede önemli, orta seviyede önemli, yüksek seviyede önemli, çok yüksek seviyede önemli olarak sıralanabilir. Olasılık değerlemesinde kullanılan beşli ölçek ise önemsiz, küçük, orta, yüksek ve çok yüksek olarak sıralanabilir[207].

Bazı riskler felaketleri içerir ve yüksek etkiye sahip olmakla beraber ortaya çıkma olasılıkları düşüktür. Diğer bazı riskler ise düşük etkiye sahip olmakla birlikte meydana gelme olasılıkları yüksektir ve toplamda önemli olabilirler. Bu faktörler ne kadar iyi belirlenirse risk tutumları da buna bağlı olarak o kadar isabetli olacaktır[208].

Risklere ait etki ve olasılıkların belirlenmesi sürecinde kullanılabilecek bilgi kaynakları eski kayıtlar, uygulamalar ile ilgili tecrübeler, ilgili basılmış kaynaklar, pazar araştırmaları, oylama sonuçları, ekonomik, teknik veya diğer modeller ve uzman görüşleri şeklinde sıralanabilir[209].

C. Risk Matrisi (Haritası)

Nitel veya nicel değerlendirme teknikleri yardımıyla olasılık ve etki boyutuyla değerlendirilen risklerin olasılık ve etki sonuçları risk matrisi (haritası) ile gösterilir.

Risklerin olasılık ve etki sonuçlarının birleştirilmesi işlemi basit ortalama veya ağırlıklı ortalama ile gerçekleştirilir. Basit ortalamada olasılık ve etki sonuçlarının toplamları ikiye bölünür. Etki faktörünün daha önemli olduğunun düşünülmesi ağırlıklı ortalamayı gündeme getirmiştir. Hesaplamada etki faktörünün ağırlığı daha fazladır. Örneğin etki faktörü 1.2 ile çarpılarak ortalamaya dahil edilir. Birleştirme işleminin alternatifi, olasılık ve etki sonuçlarının 9'lu matris üzerinde ayrı ayrı gösterilmesidir[210].

---

[206] El-Dine Dani Saad, **a.g.e.,** s. 242.
[207] Sobel, **a.g.e,** s. 6.07.
[208] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 150.
[209] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 39.
[210] Sobel, **a.g.e,** s. 6.10-11.

Tablo 5: Olasılık ve Etkinin Ayrı Gösterimi

6 Yüksek Etki / Düşük Olasılık	8 Yüksek Etki / Orta Olasılık	9 Yüksek Etki / Yüksek Olasılık
3 Orta Etki / Düşük Olasılık	5 Orta Etki / Orta Olasılık	7 Orta Etki / Yüksek Olasılık
1 Düşük Etki / Düşük Olasılık	2 Düşük Etki / Orta Olasılık	4 Düşük Etki / Yüksek Olasılık

Kaynak: Paul Sobel, Auditor's Risk Management Guide Integrating Auditing and ERM, s. 6.11.

İfade edilen kriterlere göre risk değerlemesi yapılır ve bunun sonucunda sıralanan riskler, risk matrisi (haritası) aracılığıyla toplu bir şekilde gösterilebilirler. Risk matrisi, yatay ekseni risklerin olasılık boyutunu dikey ekseni ise etki boyutunu gösteren bir grafik şeklindedir.

Risk matrisi, risk çalıştayı sürecinde gerçekleştirilen oylama sonuçlarına göre yapılır. Risk çalıştayları günümüzde genellikle bilgisayar yazılımları desteğiyle gerçekleştirilmektedir. Uygulamada en çok tercih edilen yazılımlar "Resolver*Ballot", "OptionFinder" ve "Desk Manual" olarak bilinmekle birlikte pek çok kurum ihtiyaçları çerçevesinde özel yazılım hazırlatmakta veya MS Office Excel tabanlı küçük yazılımlarla çalışmaktadır[211].

Bilgisayar ve denetim yazılımı veya standart MS Office-Excel yardımıyla yürütülen risk çalıştaylarında ilk olarak beyin fırtınası sonucunda veya önceden hazırlanan risk listesinden 20-30 adet risk bilgisayara aktarılır. Daha sonra bu riskler olasılık ve etkilerine dikkat edilmek şartıyla oylanır[212].

Oylama genellikle elektronik araçlar yardımıyla katılımcıların görüşlerinin ana bilgisayara aktarılması şeklinde olur. Oylama sürecinden sonra bilgisayar yazılımı tarafından risklerin sıralanması otomatik olarak yapılır ve risk haritasında (matrisinde) gösterilirler. Haritalanan riskler analiz edildikten sonra risklere yönelik risk tutumlarını kapsayan bir eylem planı hazırlanır[213].

---

[211] Walker, Shenkir and Barton, **Enterprise Risk Management: Pulling it all Together,** s. 22.
[212] Resolver*Ballot Product Overwiev, http://www.resolver.ca, 17.11.2006, s. 1.
[213] **a.g.e.,** s. 1.

Tablo 6: Ayrıntılı Risk Matrisi

		Parasal Büyüklük		Olasılık				
Etki	**Kritik**	**>15m YTL**	**5**	Ek Sorun	Sorun	Kabul Edilemez	Kabul Edilemez	Kabul Edilemez
	Yüksek	**10m-15m YTL**	**4**	Kabul Edilebilir	Ek Sorun	Sorun	Kabul Edilemez	Kabul Edilemez
	Orta	**5m-10m YTL**	**3**	Kabul Edilebilir	Ek Sorun	Sorun	Sorun	Kabul Edilemez
	Düşük	**1m-5m YTL**	**2**	Kabul Edilebilir	Kabul Edilebilir	Ek Sorun	Ek Sorun	Sorun
	Önemli Değil	**<1m YTL**	**1**	Kabul Edilebilir	Kabul Edilebilir	Kabul Edilebilir	Kabul Edilebilir	Sorun
				1	**2**	**3**	**4**	**5**
				<% 10	**% 10-% 30**	**% 30-% 60**	**% 60-% 90**	**>% 90**
				Az	**Olası Değil**	**Olası**	**Yüksek Düzeyde Olası**	**Beklenen**

Kaynak: Institute of Management Accountants, Statements of Management Accounting, **Enterprise Risk Management: Frameworks, Elements, and Integration,** Institute of Management Accountants, USA, 2006, s. 23, Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 20.

Kabul Edilemez: Riski yönetmek için acil eylem gerekli
Sorun: Riski yönetmek için eylem gerekli
Ek Sorun: Yeterli kaynak varsa eylem tavsiye edilebilir
Kabul Edilebilir: Eylem gerekmez

Ayrıntılı risk matrisinde, yüksek olasılık ve etkiye sahip riskler sağ üst köşeye doğru yerleştirilir ve bu grupta genellikle temel riskler yer alır. İkincil riskler ise sol üst köşeden sağ alt köşeye doğru çizilen bir köşegen üstünde yer alırlar ve bu riskler yüksek etki-düşük olasılık, orta seviyede etki-olasılık ve düşük olasılık-yüksek etki seviyesine sahip olan risklerdir. Son olarak küçük riskler olarak ifade edilen riskler ise risk matrisinin sol alt köşesine yerleştirilirler ve düşük olasılık ve etkiye sahiptirler[214].

Risk çalıştaylarının ve direkt olarak da bu sürecin bir çıktısı olan risk matrisinin başarısını etkileyen en önemli faktör farklı alanlardan katılımcıların oranının optimum seviyede olmasıdır. Katılımcılar risk alanlarından sorumlu kişiler, işletmenin faaliyette bulunduğu alandan uzmanlar veya değerleme sürecinde tecrübesi bulunan çalışanlardan meydana gelebilir[215]. Örneğin farklı alanlardan katımcıların A Riskinin olasılık seviyesi hakkında farklı düşünmeleri normaldir. Fakat örneğin hatalı bir olasılık notunun oylama sonucunu etkilemesi, risk değerleme

[214] Sobel, **a.g.e,** s. 5.30.
[215] Sobel, **a.g.e,** s. 5.22.

faaliyetinin yanlış sonuçlanmasına neden olur. Bunun için farklı alanlardan katılımcıların sayısının optimum olması çok önemlidir[216].

İç denetçi bu sürece dahil edilmemiş risk değerlemeleri risk yönetim birimi tarafından gerçekleştirilmişse bu durumda iç denetçi, risk değerleme ve risklerin sıralama faaliyetini güvence verme fonksiyonu çerçevesinde inceler. Risk değerleme sürecinin incelenmesi sırasında iç denetçi, risk etki ve olasılıklarının ölçümünde kullanılan araçların kalitesini sorgular ve risklerin tam olarak değerlenip değerlenmediği hakkında güvence verir[217].

Bütün bunların yanısıra iç denetçi güvence verme de dahil risk değerleme sürecinde yer almadığı takdirde, en azından iç denetim planında yüksek riskli alanların dikkate alındığından emin olmak için bu sürecin bir çıktısı olan risk matrisine ulaşmalı ve bu riskleri denetim planına dahil etmelidir[218]. Ayrıca bu risk değerlemelerinden yaralanılarak iç denetim elemanlarının bireysel görev dağılımları yapılır.

2.2.4.5. Risk Tutumu

Risk değerleme sürecini izleyen aşama, KRY bileşenlerinden beşincisi, risk tutumlarının belirlenmesidir. Risk çalıştayları sonucunda ulaşılan risk matrisi-risk haritası ve risk değerlemelerine uygun olarak belirlenecek olan risk tutumları risk yönetiminin riskler karşısındaki eylem alanıdır[219].

Risk tutumunun belirlenmesini etkileyen ana faktör kurum yönetimi tarafından belirlenen risk alma istekliliği sınırıdır. Risk alma istekliliği de temelde kurumun risk arayan mı yoksa risklerden kaçan bir yapıda mı olduğuyla ilgilidir[220].

Risk değerlemeleri sonucu elde edilen veriler risk alma istekliliği ile karşılaştırılır. Öncelikli olarak önlem alınması gereken riskler belirlenir ve alternatifler dikkate alınarak risk tutumları belirlenir.

---

[216] Walker, Shenkir and Barton, **Enterprise Risk Management: Pulling it all Together,** s. 130.
[217] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 13.
[218] Beasley Mark S., Clune Richard and Hermanson Dana R., "ERM A Status Report", s. 70.
[219] Sobel, **a.g.e,** s. 5.31.
[220] Hillson and Murray-Webster, **a.g.e., s**s. 26-27.

Yönetimin risk tutumu risklerden kaçınmak, riskleri üstlenmek, riskleri kontrol etmek veya riskleri transfer etmek şeklinde olabilir[221]. Risklerden kaçınma, riske neden olan faaliyetin sonlandırılmasıdır. Bu grupta, risk alma istekliliği sınırlarının dışında yer alan riskler veya kontrol maliyetlerinin risk getirisini aştığı durumdaki riskler yer alır[222]. Risklerden kaçınma, satma: riskli bir iş biriminin satılması yoluyla elden çıkarılması; devam etmeme: riskli bir ürünün üretiminin durdurulması ve yasaklama: çalışanların önceden kararlaştırılmış riskli bir olayı almasının yasaklanması olarak ifade edilebilir[223].

Riskler, eğer risk alma istekliliği yani risk sınırları içindeyse riskin olasılık ve etki boyutunu ilgilendiren herhangi bir önlem alınmadan riskler üstlenilebilir. Diğer bir ifadeyle kabul edilebilir[224]. Riskin kabulü, aynı zamanda risklerin azaltılmasından veya paylaşılmasından sonra geriye kalan risklerin kabulünü de içermektedir[225]. Günümüz işletme içi ve dış ortam koşulları altında, çok az risk bu kategoriye girmektedir.

Risklerin kontrolü en sık karşılaşılan durumdur. Risk etkisinin kurum risk alma istekliliğini aştığı ancak yönetimin riske ait etkinin kabul edilebilir bir seviyeye indirilebileceğine dair bir inancının bulunduğu durumlarda riskler kontrol altında tutulmaya, diğer bir deyişle risklerin etki ve olasılıkları azaltılmaya çalışılır[226].

Risk olasılığının azaltılması, uygun kontroller yardımıyla olayların olumsuz etkilerinin ortaya çıkma olasılığının azaltılması anlamını taşır. Risk etkisinin azaltılması ise olayların olumsuz etkilerinin büyüklüğünün azaltılarak potansiyel kayıplarının azaltılması için gerekli kontrollerin belirlenmesi ve uygulanmasını gerektirir[227].

Risklerin olasılık ve etkisini azaltmak için alınacak önlemlerden birisi de risklerin transferi-paylaşılmasıdır. Risklere ait etkinin kurum risk alma istekliliği sınırlarını aştığı ve kurum yönetiminde, risklerin yönetilebileceğine dair bir kanının bulunmadığı fakat öte yandan kurum temel stratejileri ve hedeflerine göre bu riskli

[221] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2.
[222] Pickett and Pickett, **Auditing For Managers The Ultimate Risk Management Tool,** s. 71.
[223] Sobel, **a.g.e,** s. 2.11.
[224] HM Treasury, **a.g.e.,** s. 27.
[225] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 45.
[226] Sobel, **a.g.e,** s. 2.11.
[227] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** ss. 44-45.

faaliyetin bırakılmasının da mümkün olmadığı durumlarda kurum tarafından riskli faaliyetin kurum dışı üçüncü taraflara transferi mümkün olabilir[228]. Risklerin transferi geleneksel sigortalama faaliyeti ile gerçekleştirilebileceği gibi yeni finansal araçlar olan hedging, opsiyon ve future (gelecek) sözleşmeleri ile de gerçekleştirilebilir. Bazı faaliyetlerin dış kaynaktan temini (outsourcing) de risklerin paylaşılması-transferi sınıflamasına girmektedir[229].

Risk transferinde, riskler ortadan kaldırılmamakta veya risklerin etkisi azaltılmamaktadır. Risk sadece taraflar arasında el değiştirmektedir. Genellikle risklerin finansal etkileri transfer edilebilmektedir[230]. Kurum itibarının zarara uğraması gibi risklerin transferi mümkün değildir[231]. Örneğin perakende sektöründe, zamanında ve istenilen şartlarda teslim edilmeyen mallar için aracı firmadan zarar tazmin edilebilir fakat bu durum perakendeci firmanın satışlarının düşmesini ve belki de daha önemlisi müşterinin gözünde kaybolan imajı engelleyemez[232].

Etkin bir risk yönetimi, yönetimin seçeceği risk tutumu veya risk tutumu bileşenleri aracılığıyla risklerin olasılık ve etki derecelerinin risk sınırları içinde tutulmasını sağlar.

Risk yönetimi etkinliğine yön veren belgeler, risk çalıştayı risk değerlemeleri ve eylem planı, risk stratejilerine ilişkin dokümanlar, sigorta kayıtları, kurum dışı taraflarla yapılan anlaşmalar, diğer sözleşmeler ve geçmiş yıllar izleme raporları olarak sıralanabilir[233].

Risk tutumunun belirlenmesi süreci sonunda riskler karşısındaki alternatif risk tutumları belirlenir daha sonra kurum risk kültürüne, maliyet-fayda değerlendirme sonuçlarına ve risklerle ilgili fırsat değerlendirmelerine uygun olan tutum veya tutumlar uygulamaya konur[234]. Risk tutumlarının belirlenmesi bir yönetim faaliyetidir ve iç denetçi bu aşamada sorumluluk almamalıdır.

---

[228] Sobel, **a.g.e,** s. 2.11.
[229] Morris D. Glynis, **An Accountant's Guide to Risk Management,** Tottel Publishing, UK, 2005, s. 54.
[230] Merna and Al-Thani, **a.g.e.,** s. 44.
[231] HM Treasury, **a.g.e.,** s. 27.
[232] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 14.
[233] Buckley, **a.g.e.,** s. 17.
[234] Merna and Al-Thani, **a.g.e.,** s. 46., Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 55.

İç denetçi bu aşamada yönetime risk tutumlarına ilişkin önerilerde bulunabilir. Ayrıca risklere ilişkin mevcut ve yeni tutumların etkinliklerinin değerlendirilmesi sürecinde yönetime rehberlik edebilir[235]. Örneğin iç denetim birimi işletme faaliyetlerinin tanımlanmış olan risk alma istekliliği sınırları çerçevesinde gerçekleştirilip gerçekleştirilmediği hakkında güvence verebilir. Fakat bu sürecin yürütülmesi ve sorumluluğu üst yönetime ait olmalıdır.

2.2.4.6. Kontrol Faaliyetleri

Yönetim tarafından belirlenen kontrol, politika ve prosedürlerin uygulanmasını ifade eden kontrol faaliyetleri, riskleri belirlenen risk sınırları içinde tutabilmek ayrıca risk tutumlarının etkili yürütülüp yürütülmediğinden emin olmak için kurulur ve uygulanırlar[236]. Kontrol noktaların belirlenmesinde risk alma istekliliği seviyesi ve KRY'nin hedefleri etkin rol oynarlar.

Organizasyon genelinde uygulanabileceği gibi özel bir alana da ait olabilecek olan kontrol faaliyetleri onaylamaları, yetkileri, iptalleri, kanıtları, gözlemleri, faaliyetlerin performanslarının gözden geçirilmelerini ve varlıkların fiziksel korunmalarını içerir. Geleneksel iç denetimin finansal raporlama çerçevesinde gerçekleştirdiği kontrol faaliyetlerini KRY temelli iç denetim bütün riskleri dahil ederek genişletmiştir[237].

Genel olarak kontroller; önleyici, düzeltici, yönlendirici ve saptayıcı şeklinde sınıflandırılabilirler. Kontrol faaliyetlerinin kontrol hedeflerine göre tasarlanması gerekmektedir[238].

Önleyici kontroller istenmeyen olayın ortaya çıkma olasılığını sınırlandırmak üzere tasarlanmıştır. Düzeltici kontrol ise ortaya çıkan istenmeyen olayın sonuçlarını düzeltici önlemler alınmasını ifade eder. İstenen sonuçlara ulaşılmasından emin olmak için tasarlanmış kontrol faaliyetlerine yönlendirici kontrol denir. "Olay

---

[235] Hespenheide Eric, Pundmann Sandy and Corcoran Michael, **a.g.e.,** s. 7.
[236] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management – Integrated Framework (Executive Summary),** s. 4., Sobel, **a.g.e,** s. 2.03.
[237] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 144.
[238] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 61., HM Treasury, **a.g.e.,** ss. 28-29.

sonrası" olarak da ifade edilen saptayıcı kontroller ise istenmeyen olay sonuçlarının belirlenmesine yönelik kontrol faaliyetleridir[239].

Kontrollerin belirlenmesi sürecinde dikkat edilmesi gereken bir diğer önemli nokta da en optimum kontrol seviyesinin oluşturulmasıdır. Kontroller günlük işleyişi ve faaliyetleri engellemeyecek düzeyde esnek, ancak hedeflere ulaşılma olasılığını artıracak düzeyde de sert olmalıdır[240].

2.2.4.7. Bilgi ve İletişim

Kurum amaçlarına hizmet edecek, çalışanların ve yöneticilerin sorumluluklarını yerine getirmelerine yardımcı olacak bilgiler; tanımlanmış, iletişime hazır formatta ve istenilen zamanda hazır olmalıdır[241]. Bilgi eksikliği risklerin tanımlanması, yönetilmesi ve kontrolü süreçlerinin etkinliğini zayıflatacaktır[242].

Bilgiler iç veya dış kaynaklı olabileceği gibi nitel veya nicel özellikler de taşıyabilirler. Farklı kaynaklardan gelen, farklı özelliklere sahip, farklı departmanları ilgilendiren bütün bu bilgilerin kullanılabilir hale getirilmesi ilgili birimlere raporlanması başlıca problemdir. Bunun da çözüm yolu bütün bilgileri kapsayacak şekilde tasarlanmış ve analiz yeteneği kuvvetli bir bilgi sisteminin mevcut olmasıdır[243].

Bilgi sisteminin bir parçası olan iletişim ise bilginin organizasyon içinde aşağı doğru (yönetimin planlarından çalışanların haberdar olması), paralel (departmanlar arasında personel iletişimi) ve yukarı doğru (çalışanların yönetimi bilgilendirmesi) dolaşmasıdır[244].

İç denetçi bu aşamada raporlanan anahtar riskleri değerlendirmelidir. Değerlendirmede raporlamanın, bilgilerin ve iletişimin doğru, tam ve ilgili olup olmadığı belirlenir. Değişen risklerin raporlanma zamanlılığına, risklere neden olan

---

[239] HM Treasury, **a.g.e.,** ss. 28-29.
[240] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 25.
[241] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 68.
[242] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** s. 25.
[243] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 69.
[244] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 144.

olaylara ve kontrol hatalarına ilişkin öneriler KRY sisteminin gelişimi için bir gereklilik arzeder[245].

2.2.4.8. İzleme

Kavram olarak izleme, faaliyetlere eşlik etmek, faaliyetleri izlemek, test etmek ve gerekli kişilere rapor vermek anlamındadır. İzleme faaliyetinin amacı ise kararlaştırılan önlemlerin ve süreçlerin uygulamada gerçekleştirilip gerçekleştirilmediğinin doğrulanması, söz konusu önlemlerin ve risk tutumlarının riskleri risk alma istekliliği sınırları içinde tutabilip tutamadığının doğrulanması ve son olarak da sürekli izlemeler sonucunda belirlenen sorunlara ilişkin gerekli önlemlerin alınması faaliyetlerinden oluşur[246].

İzleme, sürekli faaliyetler veya ayrık değerlendirmeler şeklinde gerçekleştirilebilir. Kurum günlük faaliyetleri içine yerleştirilen sürekli izlemeler gerçek zamanlıdır ve değişikliklere dinamik tepki verirler. Bu nedenle ayrık değerlendirmelerden daha etkindir. Sürekli izlemelerin etkinlikleri arttıkça ayrık değerlendirmelere daha az ihtiyaç duyulur[247].

Bununla beraber KRY'nin spesifik bir faaliyet olmasından ve iç denetçilerin sahip oldukları yetenek, nitelik ve tecrübelerinden dolayı ayrık değerlendirmelere daha sık başvurulması gereken kurumlar ve sektörler de olabilir[248].

İzlemelerde sıklıkla kullanılan araçlar kontrol listeleri, anketler, iş akış şemaları ve kıyaslama teknikleridir. Sektör uygulamaları ve kurumlar arası kıyaslamalar çoklukla kullanılmaktadır[249].

İzlemelerle ilgili bir diğer önemli konu da izleme faaliyetlerinin kapsam ve sıklıklarının belirlenmesidir. İzleme faaliyetlerinin kapsamları ve sıklıkları risklerin ve risk tutumlarının önem derecesi ve risklerle ilgili kontrollerle ilişkilidir. Doğal

---

[245] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 9.
[246] Morris, **a.g.e.,** s. 254.
[247] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 80.
[248] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 144.
[249] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 83.

olarak yüksek riskli alanlar ve risk tutumları daha sık değerlendirilirken bütün olarak KRY sistemini değerlendirme faaliyeti daha az rastlanılır bir durumdur[250].

Gözden kaçırılmaması gereken ve tartışmaya açık bir nokta da iç denetçilerin izleme faaliyetlerini yerine getirirken, iç denetim birimi tarafından yürütülen bir faaliyet alanının iç denetim elemanları tarafından izlenmesinin iç denetçinin objektifliğini bozacağı hususudur[251]. Uygulamada bağımsız denetçinin KRY sisteminin etkinliğinin değerlendirdiği durumlara da rastlanmaktadır. İç denetçi ile bağımsız denetçi değerlendirmelerinin birleştirilmesi daha etkin sonuçlar doğurabilir[252].

İzleme faaliyetinin anahtar başarı faktörü izlemeleri gerçekleştiren ekibin bağımsız hareket etme kabiliyetidir. Bu çerçevede ana faaliyeti yürütenler izleme ekibinde yer almamalıdır. Eğer iç denetim birimi risk yönetimi faaliyetlerinin sorumluluğunu üstlenmişse iç denetim biriminde risk yönetimi faaliyetlerinde görev almayanlardan oluşan bir izleme ekibi oluşturulmalıdır. Diğer durumda, iç denetim biriminin risk yönetiminde danışman olarak görev aldığı, ise yine risk yönetimi faaliyetlerinde görev almayanlardan oluşan bir izleme ekibi oluşturulmalıdır.

İzleme faaliyeti, uygun kontrollerin varolduğuna ve KRY aşamalarının doğru konumlandırılıp takip edildiğine[253] ve yürütülen faaliyetlerin risk tutumu stratejileriyle uyumuna ilişkin güvence sağlar[254]. Bu sürece yön veren, istenen çalışmalara temel teşkil eden belgeler yönetim performans sonuçları, yönetim kurulu ve risk komitesi raporları, denetim komitesi toplantı tutanakları ve raporu, kontrol raporları, risk değerlemeleri ile eylem planı ve iç denetim raporu olarak sıralanabilir[255].

Ayrıca izlemeler sonucunda risk sınıflandırmalarında yanlışlıklar yapılmışsa, risklerin doğru ve tam olarak ölçümünde yaşanan sıkıntılar mevcutsa ve raporlar asıl

---

[250] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 81.
[251] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 1130, A1-1.
[252] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 82.
[253] Griffiths Phil, **a.g.e.,** s. 25.
[254] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 15.
[255] Buckley, **a.g.e.,** s. 19.

ilgili ve sorumluların eline ulaşmıyor veya raporlama kapsamında sorunlar varsa bunlar ortaya çıkar ve böylelikle gerekli önlemler alınabilir[256].

2.2.5. Organizasyonel Boyut

Risk yönetimi bütün kurumu etkiler bu yönüyle KRY kurum genelinde, departman düzeyinde, bölüm seviyesinde ve birey temelli uygulanır[257].

KRY küpünün üçüncü boyutu, KRY'nin dikey bileşenleri ve KRY'nin hedefleri ile beraber ele alınmalıdır ve bu faaliyetler kurum genelinde, departman düzeyinde, bölüm seviyesinde ve birey temelli uygulanmalıdır.

2.3. KURUMSAL RİSK YÖNETİMİ ARAÇLARI

Kurumsal risk yönetimi hakkında önceki kısımlarda yer alan açıklamalar sistemin temel çerçevesini vermektedir. Bununla beraber risk yönetiminde yer alan bazı fonksiyonların gerçekleştirilebilmesi için bir takım araçlara gerek vardır.

Kurumsal risk yönetimi sürecine destek veren pek çok teknik vardır. Bu teknikler ele alınmadan önce genelde üst çatı olarak kullanılan kontrol-risk öz değerlendirme yöntemini ele almak gerekir. Kontrol-risk öz değerlendirme yönteminin yanısıra çalıştay, görüşme ve beyin fırtınası tekniklerine de risk yönetimi sürecinde sıklıkla başvurulmaktadır. Bu teknikler kontrol-risk öz değerlendirme yöntemi kapsamında ele alınabileceği gibi ayrı birer teknik olarak da düşünülebilir. Bunların yanısıra risk kayıtlaması ve denetim evreni de risk yönetimi sürecini destekleyen araçlardır. Bu araçlara ise üçüncü bölüm dördüncü kısım olan "Risk Yönetimi Temelli İç Denetimde Planlama" başlığı altında yer verilecektir.

2.3.1. Kontrol – Risk Öz Değerlendirme

Kontrol öz değerlendirme, risk ve kontrol öz değerlendirme olarak da ifade edilebilen Kontrol-Risk Öz Değerlendirme (Control-Risk Self Assessment); risk ve kontrollerin tanımlanması, değerlemesi, ölçülmesi ve izlenmesi sürecinde yönetim tarafından kullanılan bir kurumsal yönetim aracıdır[258].

---

[256] Benson Jill, "The Importance of Monitoring", **The Internal Auditor,** August 2007, s. 85.
[257] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 14.
[258] The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note: Control and Risk Self Assessment,** The Institute of Internal Auditors-United Kingdom, UK, 1999, s. 7.

İlk olarak 1987 yılında Alberta-Gulf Canada Res. Ltd. şirketi tarafından kullanılan kontrol-risk öz değerlendirme yöntemi, temel olarak çalışanların ve yöneticilerin kıdemli bir iç denetim çalışanı rehberliğinde bir araya geldiği, kurum hedeflerine ulaşılma olasılığını etkileyen her türlü faktörün değerlendirildiği bir etkinliktir[259].

Söz konusu yöntem bir denetim aracı olarak da değerlendirilebilmekle beraber aslında yönetimin sorumluluğunda olan yönetim temelli bir araçtır[260]. Uygulamada genellikle bu yöntem üst yönetim, ortaklar, orta kademe yöneticiler, çalışma ekipleri, doğal olarak denetçiler ve son yıllarda özellikle iç denetçiler tarafından kullanılmaktadır[261].

İfade edildiği şekliyle kontrol-risk öz değerlendirme yöntemi daha çok yönetim faaliyeti olarak kullanılmakla birlikte eğer bu yöntem iç denetim birimi tarafından kullanılacaksa iç denetim biriminin yeniden yapılandırılması gerekir. İç denetim faaliyetini yürüten ekip ile değerlendirme çalışmalarını yürüten ekiplerin ayrı ekipler olması bağımsızlığa daha uygundur[262].

Bu yöntemin etkin çalışabilmesi iyi bir hazırlık yapılmasına bağlıdır. Yöntemin hazırlık safhaları hedeflerin belirlenmesi, anahtar sorunların ve planların tartışılması, kurum hedeflerinin önündeki risklerin tanımlanması, dikkate alınacak risklerin belirlenmesi, mevcut önlemlerin değerlendirilmesi, mevcut stratejide yapılacak düzeltmelere karar verilmesi ve anlaşılabilir dilde ulaşılan sonuçların ve eylem planının raporlanmasından oluşur[263].

Kontrol-risk öz değerlendirme yönteminin en belirgin özelliği çalışanların parçası oldukları sistemin performansını değerlendirmelerine karşı duyulan güvendir. Bu yöntem çalıştay, görüşme ve anket teknikleri aracılığıyla yürütülür[264].

Kontrol-risk öz değerlendirme yönteminin faydaları şu şekilde sıralanabilir[265]:

---

[259] Sawyer Lawrence B., Dittenhofer Mortimer A. and others, **Sawyer's Internal Auditing,** The Institute of Internal Auditors, 2003, ss. 421-424.
[260] Wade and Wynne, **Control Self Assessment-Chapter 1,** s. 7.
[261] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 404.
[262] The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note,** s. 14.
[263] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 92.
[264] The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note,** ss. 7-8.
[265] The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note,** s. 9., Moeller, **Sarbanes-Oxley and the New Internal Auditing Rules,** s. 156.

- Problemlerin kaynağının bulunmasına yardımcı olmak,
- Yönetimin risk yönetimi ve kontrollere ilişkin sorumluluklarını yeniden güncellemesine yardımcı olmak,
- Kurum çalışanlarının risk ve kontrollerin hedeflerini ve etkinliklerini daha iyi anlamalarını sağlamak,
- Denetimin yüksek riskli alanlara odaklanmasını sağlamak,
- Düzeltici önlemlerin sorumluluğunu ilgili faaliyet çalışanlarına aktararak önlemlerin etkinliği artırmak.

Yukarıda ifade edilen faydalara ek olarak kontrol-risk öz değerlendirme yönteminin aşağıya-yukarıya doğru ve paralel iletişimi güçlendirdiği de gözlemlenmiştir[266].

Kontrol-risk öz değerlendirme yönteminin daha etkili çalışabilmesi açısından dikkat edilmesi gereken bir takım kritik faktörler vardır. Bu faktörler sırasıyla şunlardır[267]:

- Kontrol-risk öz değerlendirme yöntemi çalıştay temelli yürütüldüğü durumlarda, çalıştaya katılacak doğru katılımcıların seçimi çok önemlidir,
- Çalışanların ve yönetimin kuruma güvenlerinin tam olması ve sonuçların uygulamaya konulacağına ilişkin inanç önemli bir rol oynar,
- Kontrol-risk öz değerlendirme yöntemi basit finansal kontrollerin yanısıra organizasyon genelindeki operasyonel kontrolleri ve risk yönetimi faaliyetlerini kapsamalıdır. Eğer bu kapsam genişliği yerleştirilemezse programın olası faydaları gerçekleşmez,
- Yöntemin başarısının temelinde kurum amaçlarının doğru anlaşılması vardır.

Kontrol-risk öz değerlendirme yönteminin çıktıları yardımıyla iç denetçi, kurum içindeki kontrol süreçleri hakkında daha fazla bilgi edinir ve bu ek bilgileri, kıt olan denetim kaynaklarını, önemli kontrol zayıflıkları olan veya yüksek risklerle

[266] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 91.
[267] The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note,** s. 10., Wade and Wynne, **Control Self Assessment-Chapter 24,** s. 388.

karşı karşıya olan iş birimlerinin veya fonksiyonlarının araştırılmasına ve bu konuda gereken testlerin yapılmasına tahsis etmek amacıyla kullanabilir[268].

Kontrol-risk öz değerlendirme yöntemi risk çalıştayı, görüşme ve beyin fırtınası formatında kullanılabilmekle birlikte ABD uygulamasında genellikle risk çalıştayı formatının % 70 oranında ve görüşme formatının ise % 30 oranında tercih edildiği görülmektedir[269].

2.3.1.1. Çalıştay

Çalıştay, kontroller ve riskler hakkında bilgi ve verilerin direkt olarak kurumu temsil kabiliyeti olan farklı birimlerdeki çalışanlardan toplanması ve bir eylem planına ulaşılması amacıyla organize edilen bir faaliyettir[270].

Çalıştaylar hakkında 1997 yılında İngiltere'de yapılan araştırmada uygulamada çoğunlukla 10-12 kişilik katılımcıyla yapılan çalıştayların ortalama 3-4 saat sürdüğü belirlenmiştir[271]. Uygulamada çoğu zaman yarım gün süren çalıştayların hazırlık faaliyetleri ise uzun zaman almaktadır.

Kontrol-risk öz değerlendirme yöntemi temelli düzenlenen çalıştaylar aşağıdaki gibi beş başlıkta toplanabilir[272]:

- Hedef temelli (kontrol ve artık risklerle ilgili),
- Risk temelli (riskler ve kontrollerle ilgili),
- Kontrol temelli (geleneksel denetim faaliyetlerini içerir),
- Süreç temelli (işletme süreçleri ve toplam kalite yönetimi ile ilgili),
- Departman temelli (yetenekler ve engeller ile ilişkili).

Çalışmanın kapsamı gereği burada sadece risk temelli çalıştaylar ayrıntılı bir şekilde incelenmektedir.

---

[268] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2120.A1-2.
[269] Vallabhaneni Rao S., **Wiley CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** John Wiley & Sons, USA, 2005, s. 98.
[270] The Institute of Internal Auditors, Professional Practices Pamphlet: A Perspective on Control-self Assessment, USA, 1998, s. 2.
[271] Wade and Wynne, **Control Self Assessment-Chapter 6,** s. 98.
[272] Vallabhaneni, **Wiley CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** s. 98.

Risk yönetimi temelli düzenlenecek olan bir çalıştayın hazırlık aşaması çalıştay konusunun belirlenmesini, teknik araştırmayı, çalıştay aşamalarının tasarlanmasını ve çalıştay ajandasının hazırlanmasını içerir[273].

Çalıştayların, dengeli ve doğru değerlendirme sonuçlarına ulaşmasını etkileyen en önemli faktörlerden birisi bütün kurumun doğru oranda temsil edilmesidir. Çalıştay sürecini etkileyen diğer bir faktör de çalıştay öncesinde çalıştay aşamaları ve içerik hakkında katılımcıları bilgilendirmedir. Uygulamada genellikle ön bilgilendirme çalıştay öncesinde düzenlenecek bir toplantı ile yapılmaktadır[274].

Risklerin tanımlanması, değerlendirilmesi ve bunun soncunda oluşturulan risk tutumlarını içeren çalıştay faaliyeti sonucunda çalıştay raporu hazırlanır. Çalıştay raporu içerik olarak risk kayıtlamasını kapsamaktadır. Fakat risk kayıtlaması tam olarak çalıştay raporunu kapsamamaktadır. Genellikle iç denetçi tarafından düzenlenen çalıştaylara ait raporun çalışma kâğıtları arasına eklenmesi iç denetçiye kendisini savunması açısından bir kanıt-dayanak sağlar[275].

Çalıştayın iç denetçi tarafından düzenlendiği durumlarda denetçi bir denetim görevini yerine getirir gibi davranmaktan ziyade bağımsız bir hakem veya lider gibi davranmalıdır ve denetçinin amacı çalıştayın amacı ile paralel olmalıdır[276].

Çalıştay sonunda katılımcıların üzerinde uzlaştıkları bir risk sıralaması ve risk haritası hazırlanır. Uygulamada sıklıkla kullanılan bir şablon rehberliğinde bu çalışmanın amacına ve içeriğine uyarlanmış bir risk değerleme çalıştayı örneği aşağıdaki gibidir[277]:

- ✓ **Amaç**

Bu risk değerleme yönergesi kritik işletme süreçlerinin ve iç kontrollerin tanımlanması ve belgelendirilmesi amacıyla tasarlanmıştır. Sarbanes-Oxley yasasına uyum amaçlı düzenlenen bu risk çalıştayı kritik işletme süreçlerinin sınıflandırılmasına ve sıralanmasına yardımcı olacaktır. Üst yönetimle yapılan toplantılarla bütünleştirilecek olan bu çalıştay, kurum süreçleri arasında anahtar

[273] Wade and Wynne, **Control Self Assessment-Chapter 8,** s. 135.
[274] Wade and Wynne, **Control Self Assessment-Chapter 8,** s. 137.
[275] Pehlivanlı Davut, "Kurumsal Risk Yönetimi Temelli İç Denetim Araçları", **İç Denetim,** Bahar 2007, Sayı 18, s. 29.
[276] Griffiths Phil, **a.g.e.,** s. 58.
[277] Protiviti Knowledge Leader, **Risk Assessment Instruction,** www.knowledgeleader.com, 05.06.2007.

süreçleri yürütenlerin de dahil olduğu organizasyon genelinde bir uzlaşma sağlanmasına katkıda bulunacaktır.

- ✓ **Hedef**

Risk çalıştayına katılacak olanlardan alınacak geri beslemelerle işletmedeki kritik süreçlerin tanımlanılması ve sıralanması amaçlanmaktadır. Bu çerçevede katılımcılardan işletme süreçleri içerisinde yer alan en kritik 15 süreci tanımlamaları ve daha önceden belirlenmiş kriterlere göre sıralandırmaları beklenmektedir. Katılımcılardan alınacak olan listeler birleştirilir ve kurum genelini kapsayan bir risk listesi oluşturulur. İç denetim birimi çalıştayı izleyen iki hafta içinde sonuçları tartışmak ve üzerinde fikir birliğine varılmış, sınıflandırılmış ve sıralanmış bir listeye son halini vermek için bir toplantı düzenler. Bundan sonraki üç aylık süreç içindeyse iç denetim birimi süreçlerin belgelendirilmesini ve imkânlar dahilinde her kritik sürece ilişkin kontrolleri düzenler.

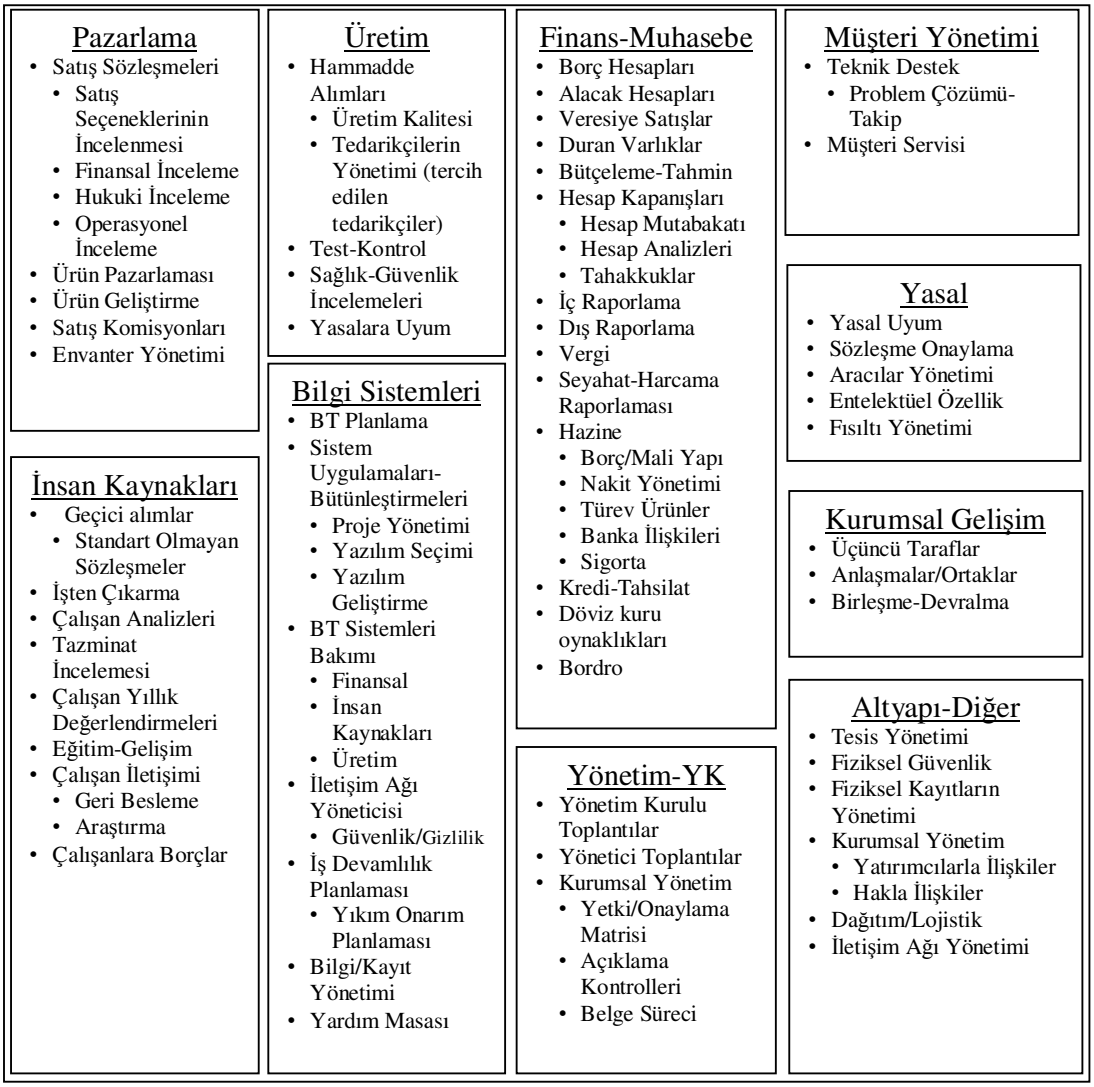
- ✓ **Süreç**

İşletmeye ait süreç listesi, izleyen sayfada süreç evreni isimli tabloda yer almaktadır. Bu liste seçilecek olan 15 risk için bir temel oluşturmaktır. Bu listede yer almayan riskler de oluşturulacak olan risk listesine eklenebilir.

- ✓ **Risk Haritası**

Riskler sınıflandırılırken 1) işletmeye ve finansal performansa etkisine, 2) süreçlerin ve kontrol zayıflıklarının olasılıklarına dikkat edilir. Sonuç olarak da risk matrisine yerleştirilir.

Tablo 7: Süreç Evreni



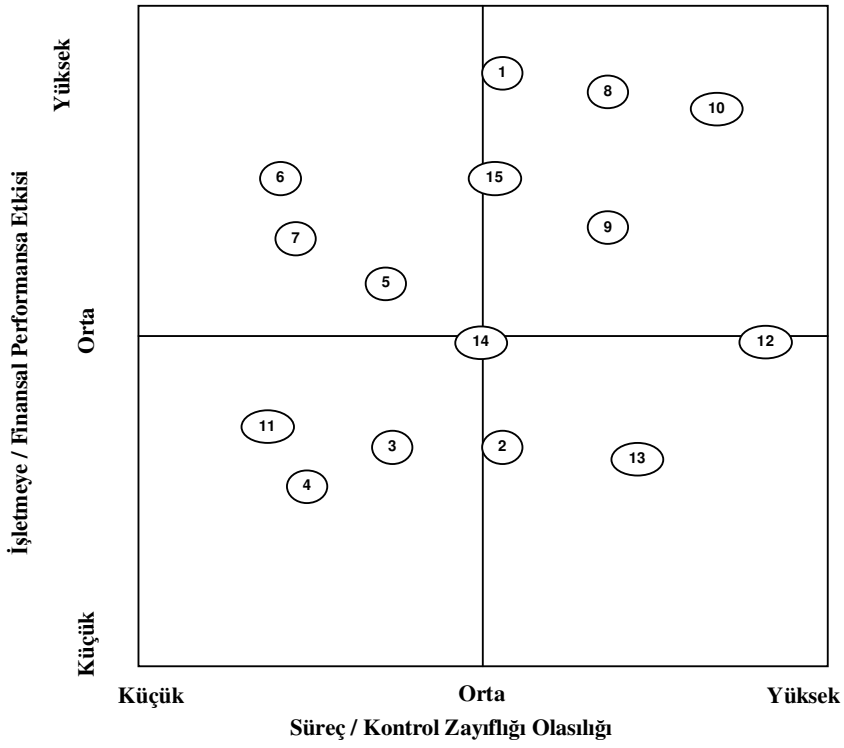
Kaynak: Protiviti Knowledge Leader, **Risk Assessment Instruction,** www.knowledgeleader.com, 05.06.2007.

Aşağıda oluşturulan liste 15 örnek kritik süreci ve her sürecin işletmeye/finansal performansa etkisi ve süreç/kontrol zayıflıklarının olasılıkları açısından sıralanmıştır. Bu listenin hazırlanması aşamasında çalıştay katılımcıları süreç evreninde olmayan riskli faaliyetleri de listeye ekleyebilirler.

1. Satış Sözleşmeleri
2. Hammadde Alımları
3. Alacak Hesapları
4. Kredi - Tahsilat
5. Sipariş Alım Süreci

6. Sağlık Değerlemeleri
7. Duran Varlıklar
8. Envanter Yönetimi
9. Nakit Yönetimi - Hedge
10. Yasal Uyum
11. Tesis Yönetimi
12. Dağıtım - Lojistik
13. İletişim Ağı Güvenliği - Gizlilik
14. Sigorta - Risk Yönetimi
15. Kurumsal Yönetim

Olasılık ve etkileri bakımından sıralanan riskler risk haritasına yerleştirilerek çalıştay son bulur. Risk haritasında 10 numara ile gösterilen "Yasal Uyum" riski çalıştay sonuçlarına göre en kritik risktir. 11 numaralı "Tesis Yönetimi" ise seçilen riskler arasında göreceli olarak en az öneme sahip risktir.



Şekil 7: Risk Haritası

Kaynak: Protiviti Knowledge Leader, **Risk Assessment Instruction,** www.knowledgeleader.com, 05.06.2007.

Çalıştay sonunda, belirlenen ve üzerinde uzlaşılan verilerin kayıt edilmesi gerekmektedir. Risk haritasının yanısıra bir de risk kayıtlamalarında kullanılacak, her

bir riske ait risk kartları oluşturulmalıdır. Bu kartlarda risk tanımı, riskten sorumlu personel, riskin etki ve olasılığı sonuç olarak toplam puanı, risklere karşı halen yürütülmekte olan yönetim faaliyetleri ile eylem planı ve zamanlama yer alabilir. Sözkonusu kart iç denetçi tarafından düzenlenecek bir çalışma kâğıdı olarak kabul edilebilir.

Tablo 8: Risk Kartı

<table>
<tr><td>Tanım</td><td>Risk Sahibi</td></tr>
<tr><td>Kabul edilen risk tanımı</td><td>Riskten sorumlu personel</td></tr>
<tr><td>Etki</td><td>Puanı</td></tr>
<tr><td>Riskin işletmeye etkisi</td><td rowspan="3">Toplam risk skoru</td></tr>
<tr><td>Olasılık</td></tr>
<tr><td>Olasılık % cinsinden</td></tr>
<tr><td>Güncel Yönetim Faaliyetleri</td><td>Öncü Uygulamalar</td></tr>
<tr><td>Risklerin yönetimi için yürütülen faaliyetler</td><td>Sektörel bazda uygulanan yöntemler</td></tr>
<tr><td colspan="2">Eylem Planı ve Zamanlama</td></tr>
<tr><td colspan="2">☐ Kaçınma
☐ Üstlenme
☐ Kontrol Etme
☐ Transfer</td></tr>
</table>

2.3.1.2. Görüşme ve Beyin Fırtınası Yöntemi

Genellikle bire bir görüşme tarzında yapılan görüşme yöntemlerinden işletme stratejilerinin ve hedeflerinin belirlenmesi, risklerin tanımlanması ve değerlendirilmesi aşamalarında sıklıkla yararlanılmaktadır. Görüşmenin akışına uygun olarak görüşmeyi yapan tarafından mevcut sorular artırılıp azaltılabilir.

Risklerin tanımlanması ve değerlendirilmesi sürecinde beyin fırtınası yönteminden de yararlanılabilir. Beyin fırtınası çalışma ekibinin bir araya getirilerek

riskler hakkında özgür bir ortamda tartışmalarının sağlandığı ve sonuçta tanımlanan risklerin değerlemesinin ve sıralamasının yapıldığı bir yöntemdir[278].

2.4. KURUMSAL RİSK YÖNETİMİ SİSTEMİNİN SINIRLARI

Kurumsal risk yönetimi çerçevesinin oluşturulabilmesi ve etkin çalışabilmesi üst yönetimin desteğine, kurumun risk yönetimi felsefesine, risk alma istekliliğine, KRY sisteminin kapsamına ve bu sistemi destekler nitelikteki bilgi altyapısının varlığına bağlıdır[279]. Eğer üst yönetim desteklemiyorsa veya kısıtlı-yetersiz bir destek veriyorsa iç denetçi sistemin işlemesi için gerekli verilere ulaşamayacak, risk çalıştaylarını düzenleyemeyecek ve diğer faaliyetleri gerçekleştiremeyecektir.

Yönetimin desteğinin ötesinde KRY çok iyi tasarlanmış ve yürütülmüş olsa da sistemin sınırlarından ötürü makul düzeyde güvence vermenin ötesine geçilemeyebilir. Kurumsal risk yönetiminin en büyük kısıtı çalışma alanı olan risklerin belirsizlik ortamının bir sonucu olmasıdır. Bilindiği gibi riskler, geleceğin belirsizliğinden kaynaklanmaktadır ve bu belirsizliği ortadan kaldırmanın imkânı yoktur. Bu şartlar altında, hem iç denetçi tarafından sistemin etkin çalışıp çalışmadığı hakkında hem de KRY sorumluları tarafından riskler hakkında mutlak güvence verilemez.

Sistemin önündeki bir diğer kısıtta; risklerin hızlı bir şekilde değişebilmesi bundan dolayı daha önceden tanımlanan olasılık ve etkilerin geçerliliğini kaybetmesidir[280]. Bu durum tarihsel verilerle hareket etmeyi zorlaştırmakta ve sistemin hali hazırda sahip olduğu verileri anlamsızlaştırabilmektedir.

KRY'nin önündeki sınırların bir diğeri de işletme kararlarının alınması sürecinde insan doğasından kaynaklanabilecek zayıflıklardır. Kararlar insan yargılarıyla, eldeki veriler ışığında ve iş hayatının baskı dolu sürecinde alınmaktadır. Bu durum da kararların güvenilirliğini zayıflatabilir[281]. Ayrıca üst yönetim veya diğer kurum çalışanlarının sistemi yanlış yönlendirmeleri sonucu riskli alanlar

---

[278] El-Dine Dani Saad, **a.g.e.,** s. 237.
[279] Booker Fay M., **a.g.e.,** s. 6, Walker, Shenkir and Barton, **Enterprise Risk Management: Pulling it all Together,** s. 18, Institute of Management Accountants, Statements of Management Accounting, **Enterprise Risk Management: Frameworks, Elements, and Integration,** s. 15.
[280] The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** Chapter 5, s. 134.
[281] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** s. 89.

belirlenmemiş olabilir. Doğal olarak da risk yönetimi sisteminin etkin çalışması mümkün olmayabilir.

Sistemin etkin işlerliği, belirlenmiş risklerin organizasyona etkilerinin objektif bir şekilde tespitine bağlıdır. Günümüz rekabet ortamı ve işletmelerin küresel düzeyde rekabete ve küresel ekonomik gelişmelere kırılgan hale gelmesi karşılaşılan risklerin hem adet olarak artmasına hem de çeşitlenmesine neden olmuştur. Çok sayıda riske ait etkinin objektif olarak belirlenmesi de çok önemli bir problemdir. Uygulamada bu sorun, çalıştay sonucunda belirlenen risklerin bir kısmının "filtrelenmesi", kurum risk alma istekliliği çerçevesinde gözardı edilmesi, ile çözülmektedir[282].

İfade edilen sınırların yanısıra KRY sistemin etkinliği aşağıda sıralanan faktörlerle yüksek düzeyde bir ilişki içindedir[283]:

- KRY uygulamalarının sorumluluğunu üstlenecek personelin bağımsız çalışabilme yeterliliği,
- Görev ve sorumlulukların açık bir şekilde tanımlanması ve ayrıştırılması,
- Teorik yaklaşımlar yerine işletme ve sektörün ihtiyaçlarına uygun çözümler üretilmesi,
- KRY'nin tehditler kadar fırsatlara da odaklanması,
- Risk yönetimi sürecinin etkinliğinin izlenmesi amacıyla denetim mekanizmasının kurulması.

[282] Page Michael and Spira Laura F., **The Turnbull Report, Internal Control and Risk Management: The Developing Role of Internal Audit,** s. 25.
[283] TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **a.g.e.,** ss. 8-9.

III. BÖLÜM
KURUMSAL RİSK YÖNETİMİ TEMELLİ İÇ DENETİM FAALİYETİNİN PLANLANMASI, YÜRÜTÜLMESİ VE RAPORLANMASI

Denetim yaklaşımlarına, genellikle denetimin odak noktasının ismi verilmektedir. Denetimde odak noktanın, kontroller üzerinde olduğu dönem "kontrol odaklı denetim" olarak ifade edilmiştir. Yaşanan değişim sonrasında odak noktanın risklere kayması, 2004 yılında COSO tarafından Kurumsal Risk Yönetimi çerçevesinin yayınlanması ve iç denetimin risk yönetimi süreciyle bütünleştirilmesi çabaları kavram olarak "Kurumsal Risk Yönetimi Temelli İç Denetim"in ortaya çıkmasına zemin hazırlamıştır.

Kurumsal risk yönetimi temelli iç denetim, kurumların risk karakteristiklerinin belirlenmesi ve değerlendirilmesi, denetim sürecinin kurum risk sıralamasına (risk matrisi veya risk haritası ile uyumlu) uygun olarak tasarlanması ve sınırlı denetim kaynaklarının risk değerlendirilmesine uygun olarak dağıtımına dayanan etkinliği artırmayı ve risk yönetimi sisteminin etkinliğinin denetimini hedefleyen bir denetim yaklaşımıdır. Bu yaklaşımda iç denetim birimi, risk yönetimi faaliyetlerine yönelik güvence veya danışmanlık hizmetlerini yürütmektedir.

Kurumsal risk yönetimi ilkelerinin yön verdiği kurumsal risk yönetimi temelli iç denetim, geleneksel denetim fonksiyonlarının yanısıra, genel olarak kurum risk yönetimi sisteminin riskleri, daha önceden belirlenmiş olan risk alma istekliliği sınırları çerçevesinde, istenildiği gibi, yönetip yönetemediğine ilişkin güvence sağlar[284]. Denetim faaliyeti sonunda risk yönetimi süreçleri açısından belirlenen mevcut durum ile arzu edilen durum karşılaştırması risk yönetimi sisteminin aksaklıklarının giderilmesine yardımcı olacaktır[285].

[284] The Institute of Internal Auditors – UK & Ireland, **Position Statement - Risk Based Internal Auditing,** s. 1.
[285] Sobel, **a.g.e,** s. 11.02.

Tablo 9: COSO KRY Çerçevesi - KRY Temelli İç Denetim Bağlantıları ve İç Denetim Aşamaları

COSO KRY Çerçevesi	KRY Temelli İç Denetim ve Bağlantılar	Denetim Aşamaları
Kontrol Ortamı	Kurum ile ilgili verilerin girdisi	Kurum Yapısının Anlaşılması ve Denetimde Planlama
Hedeflerin Belirlenmesi	Kurum hedefleri Kurum iş modelinin ve risk alma istekliliği sınırlarının anlaşılması	
Olay-Risk Tanımlama	Risklerin belirlenmesi ve tanımlanması süreci ve risk kayıtlaması için ilk veriler	
Risk Değerleme	Risklere ait olasılık ve etki değerlendirmeleri Risklerin sıralanması Risk kayıtlaması	
Risk Tutumu	Risk alma istekliliği sınırları çerçevesinde risk tutumları Denetim evreninin tasarlanması için temel veriler	
Kontrol Faaliyetleri	Test aşamaları	Denetimin Yürütülmesi
Bilgi ve İletişim	Sistemin işlerliğine yönelik bilgi ve iletişim	Denetimde Raporlama
İzleme	İzleme ve takip süreci	

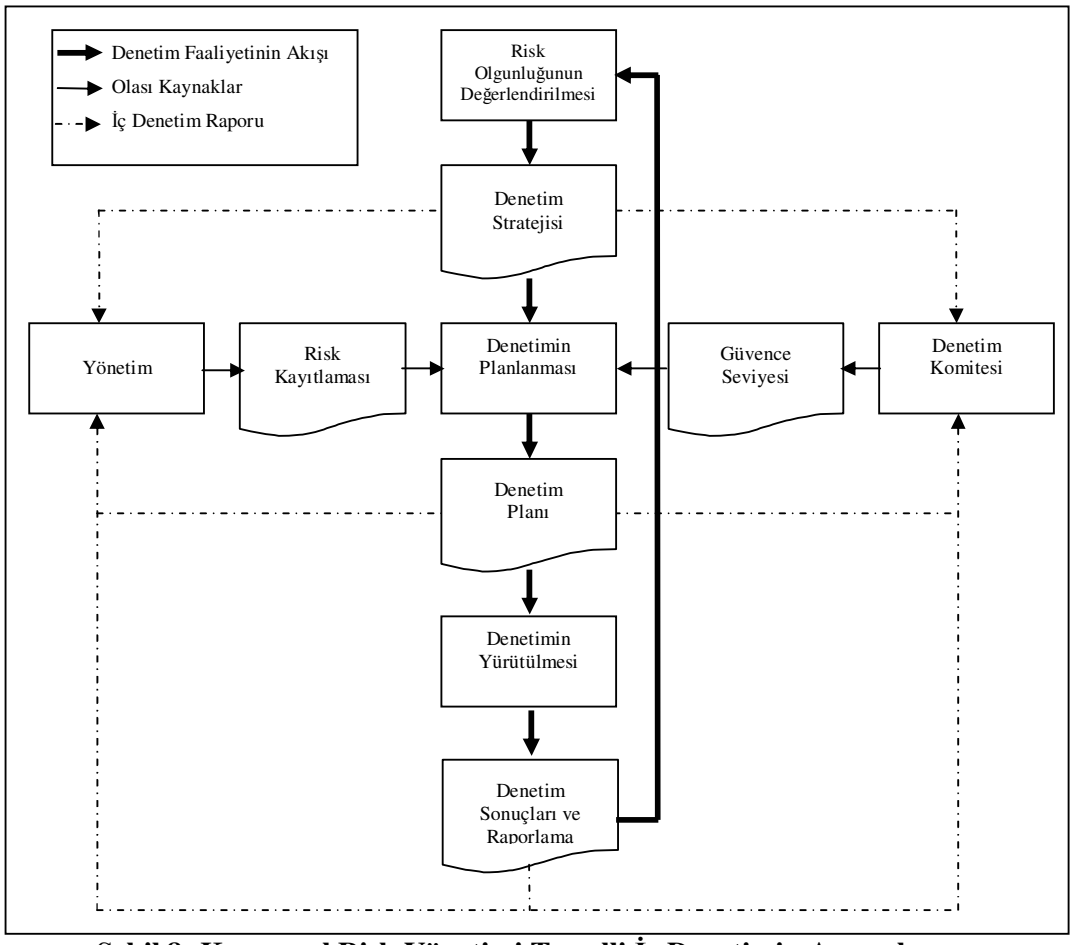
Kaynak: Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005, s. 14.10'dan alınarak geliştirilmiştir.

Tabloda yer aldığı şekliyle kurumsal risk yönetimi temelli çalışan iç denetim sistemi KRY bileşenlerinin iç denetim aşamalarına paralel olarak birleştirilmesinden meydana gelir. KRY bileşenlerinden kontrol ortamı, hedef belirleme, olay-risk tanımlama, risk değerleme ve risk tutumu aşamaları denetimde kurum yapısının anlaşılması ve denetimin planlanması ile örtüşmektedir. KRY bileşenlerinden altıncısı olan kontrol faaliyetleri genel anlamda denetim faaliyetlerinin yürütülmesi ile paralellik gösterirken bilgi ve iletişim ile izleme süreci ise iç denetimde raporlama süreci ile paralellik gösterir.

3.1. RİSK YÖNETİMİ TEMELLİ İÇ DENETİMİN AŞAMALARI

Birleşik Krallık-İrlanda İç Denetçiler Enstitüsü açıklama rehberinde yer aldığı şekliyle kurumsal risk yönetimi temelli iç denetimin aşamaları; risk olgunluğunun değerlendirilmesi, denetim stratejisi çerçevesinde denetimin planlanması, bireysel

denetim görevinin gerçekleştirilmesi ve son olarak denetimin raporlanması şeklinde sıralanmıştır[286].



Şekil 8: Kurumsal Risk Yönetimi Temelli İç Denetimin Aşamaları

Kaynak: The Institute of Internal Auditors - UK and Ireland, **An Approach to Implementing Risk Based Internal Auditing,** Institute of Internal Auditors - UK and Ireland, December 2005, s. 7.

Risk yönetimi olgunluğunun değerlendirilmesi ve risk kayıtlaması direkt olarak risk yönetimi süreci ile olan bağlantı noktalarıdır. Ayrıca risk kayıtlaması aracılığıyla risk ve denetim evreni de risk yönetimi sisteminin verileri ile desteklenmektedir.

[286] The Institute of Internal Auditors – UK & Ireland, **Position Statement - Risk Based Internal Auditing,** UK, August 2003, s. 1.

Şekil 8'de gösterilen kurumsal risk yönetimi temelli iç denetim aşağıdaki aşamalardan meydana gelir[287]:

- Kurumsal risk yönetiminin de başlangıç aşaması olan kurum kontrol ortamının ve kurum hedeflerinin incelenerek, kurumsal risk yönetimi hedeflerinin belirlenmesi aşaması ile paralel, kurum iş süreçlerinin anlaşılması faaliyetlerini kapsayan *kurum yapısının anlaşılması ve risk yönetimi olgunluğunun değerlendirilmesi,*
- Denetim stratejisi çerçevesinde risk kayıtlamasının hazırlanması ve gerekli güvence seviyesinin belirlenmesi süreçlerini kapsayan, denetim planının hazırlanması ile plan hakkında denetim komitesinin ve yönetimin görüşlerinin alınması aşamalarından oluşan *denetimin planlanması*,
- Denetçi görüşüne ulaşabilmek için denetimin yürütülmesi açısından genel denetim planına paralel bireysel denetim planının yapılması, denetim faaliyetlerinin gerçekleştirilmesini kapsayan *denetimin yürütülmesi,*
- Yönetimin gözetiminde risk ve denetim evrenindeki gerekli güncelleştirmelerin yapılması, son olarak bireysel denetim sonuçlarından hareketle denetim komitesine ve yönetime sunulacak olan denetim faaliyet özetinin ve raporunun tamamlanması aşamalarını kapsayan *denetimin sonuçlandırılması ve raporlanması*.

Şekilde yer alan kalın oklar (➡) denetim faaliyetinin temel akışını gösterirken, normal kalınlıktaki oklar (→) iç denetim faaliyetine destek olan kurumsal risk yönetimi sistemi çıktılarını denetim açısından ise kaynakları-girdileri gösterir. Kesik çizgili oklar ise (⇢) hazırlanacak iç denetim raporunun yayınlanmadan önce, organizasyon yapısı içinde, hangi birimlerin görüşlerinin alınacağını, raporun sorumluluğunun kimde olduğunu ve hazırlanacak denetim raporunun kurum denetim stratejisi ile uyumlu olması gerekliliğini göstermektedir.

[287] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 26, Gupta, **a.g.e.,** s. 144., Griffiths Phil, **a.g.e.,** ss. 73-145., The Institute of Internal Auditors – UK & Ireland, **An Approach to Implementing Risk Based Internal Auditing,** Institute of Internal Auditors - UK & Ireland, December 2005, s. 7.

3.2. KURUM YAPISININ ANLAŞILMASI VE RİSK YÖNETİMİ OLGUNLUĞU

Kurum yapısının anlaşılması ve risk yönetimi olgunluğunun belirlenmesi aşaması, denetimin kapsamının ve denetçinin verebileceği hizmetlerin çerçevesinin belirlenmesi için bir ön hazırlık safhası olarak kabul edilebilir.

3.2.1. Kurum Yapısının Anlaşılması

Kurum stratejilerinin, amaçlarının ve hedeflerinin bilinmesi kurumun nasıl bir çevrede, hangi sektörde faaliyette bulunduğunun, ne tür zorluklarla karşılaştığının anlaşılması, risk tanımlamalarının ve risk yönetiminin etkin işleyebilmesi için temel şarttır[288].

Denetim planlamasının ilk adımı olan kurum yapısının anlaşılması aynı zamanda kurumsal risk yönetimi bileşenlerinden ilk ikisi olan kurum kontrol ortamı ve hedeflerin belirlenmesi süreci ile paralellik göstermektedir ve bu durum risk yönetimi temelli çalışan iç denetim sistemi için temel koşuldur.

Kurum yapısının anlaşılmasının yanısıra denetim planının istenen hedefe ulaşabilmesi planlama öncesinde yönetimin amaçlarını ve isteklerini netleştirmesine, yönetimin aktif işbirliği ve iletişimine bağlıdır[289].

3.2.2. Risk Yönetimi Olgunluğu

Risk yönetimi olgunluğu, kurumun riskleri anlama ve risk yönetimini uygulama derecesi olarak ifade edilebilir[290] ve risk yönetimi sisteminin stratejiler, süreçler, çalışanlar, teknoloji ve iletişim açısından incelenmesi ile belirlenir[291]. Planlama aşamasında risk yönetimi olgunluğunun değerlendirilmesi, denetçinin risk yönetimi çıktılarına ne kadar güvenebileceği ve denetçiye bunları kullanıp kullanamayacağı konusunda bir değerlendirme yapma fırsatı verir. Her bir olgunluk seviyesi için iç denetçinin risk yönetimi sisteminin verilerini kullanması farklı olmakta ve bu da iç denetçinin iş yükünü etkilemektedir.

---

[288] Buckley, **a.g.e.,** s. 31.
[289] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 600.
[290] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 23.
[291] Sobel, **a.g.e,** ss. 2.12-13.

Beş seviyeden oluşan risk yönetimi olgunluğu; bütünleştirilmiş riskler, yönetilebilir riskler, tanımlanmış riskler, risklerin farkındalığı ve saf riskler olarak adlandırılabilir[292].

Bütünleştirilmiş risk seviyesi, risk yönetimi ve kontrollerin kurum kültürüne ve faaliyetlere yerleştirilmiş olduğunu ifade eder. Bu ortamda iç denetçi, yönetimin risk değerlemelerini ve risk yönetiminin bütün çıktılarını kullanabilir[293]. Bu durum denetimin planlaması aşamasında gerekecek olan güvenilir risk kayıtlamasının mevcut olduğu anlamına gelir[294].

Risk olgunluğunun ikinci aşaması olan risklerin yönetilebilir olması, ilgili kurumda risk yönetim sisteminin faal olduğunu ifade etmektedir. Bütünleştirilmiş risk seviyesinde olduğu gibi bu seviyede de iç denetçi yönetimin risk değerlemelerini kullanabilir[295]. Fakat bu aşamada her zaman iç denetçinin ulaşabileceği güvenilir bir risk kayıtlaması mevcut olmayabilir. İç denetçi mevcut risk kayıtlamalarını ve ilgili risk yönetimi çıktılarını inceler ve kullanıp kullanmayacağına karar verir.

Kurum stratejilerinin, politikalarının ve risk alma istekliliğinin belirlenmiş olduğu aşama risklerin tanımlanmış olduğu risk olgunluk seviyesidir. Yönetim tarafından derlenmiş bir risk listesi bulunmaktadır ve denetçi yapılan incelemeler sonunda bu listeye dayanarak risk kayıtlamasını oluşturup oluşturamayacağına karar verir[296].

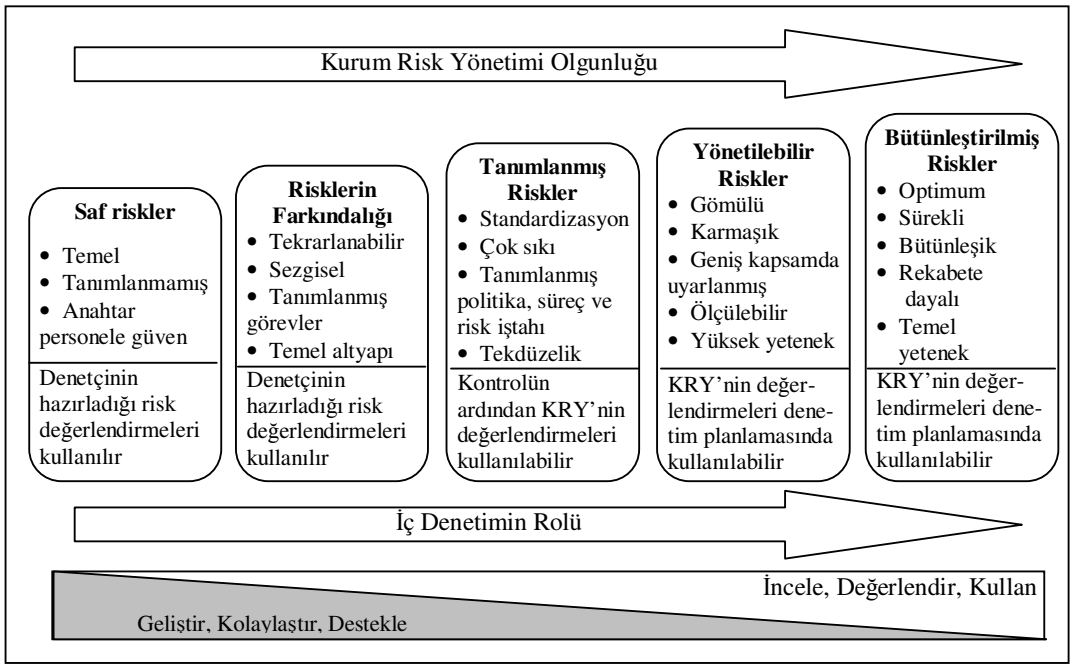
Risklerin farkındalığı aşamasında, kullanılabilir bir risk kayıtlaması mevcut değildir sadece bazı yöneticiler tarafından kendilerini ilgilendiren risk tanımlamaları yapılmıştır[297]. İç denetçi danışman sıfatıyla kurumsal risk yönetiminin kurulması aşamasında yönetime yardımcı olabilir[298]. Sonuç olarak bu seviyede iç denetçi tarafından kullanılabilecek mevcut, sürekli ve düzenli herhangi bir doküman veya risk kayıtlaması bulunmamaktadır.

---

[292] The Institute of Internal Auditors – UK & Ireland, **Position Statement - Risk Based Internal Auditing,** s. 3.
[293] Buckley, **a.g.e.,** s. 7.
[294] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 24.
[295] Buckley, **a.g.e.,** s. 7.
[296] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 24.
[297] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 24.
[298] Cain Jackie, "An Approach to Implementing Risk Based Internal Auditing", The Institute of Internal Auditors UK & Ireland, **South-West District Event,** 15 March 2006, s. 16.

Risk yönetimine ilişkin kurum düzeyinde kabul edilmiş hiçbir yaklaşımın bulunmadığı ve kurumun karşılaştığı risklere ilişkin hiçbir çalışmanın yapılmadığı aşama risklerin saf haliyle bulunduğu aşamadır. Risklerin farkındalığı aşamasında olduğu gibi iç denetçi yönetimin ihtiyaçları doğrultusunda faaliyette bulunabilir[299]. Bu aşamada tanımlanmış bir risk alma istekliliği sınırı ve risklere ilişkin diğer bilgiler bulunmamaktadır[300].

Şekil 9'da kurum risk yönetimi olgunluğuna paralel olarak iç denetimin olası rolleri ve her bir risk yönetimi olgunluk seviyesinin temel karakteristikleri gösterilmektedir.



Şekil 9: Risk Yönetimi Olgunluğu ve İç Denetimin Rolü

Kaynak: Norman Buckley, **It's a Risky Business: a Practical Guide to Risk Based Auditing,** The Chartered Institute of Public Finance and Accountancy (CIPFA), UK, 2005, s. 32'den alınarak güncelleştirilip geliştirilmiştir.

Kurum risk yönetiminin olgunluk seviyesi iç denetimin çalışma alanını ve danışmanlık ve güvence fonksiyonlarının derecesini belirler. Kurum risk yönetiminin olgunluk seviyesi yüksekse, bütünleştirilmiş riskler, kurumun karşılaştığı risklere ilişkin sağlanan veriler gerekli değerlendirmelerin ardından direkt olarak denetim planlamasında kullanılabilir. Bu durumun tersi yani risk yönetimi olgunluk seviyesinin en düşük olduğu seviyede, saf riskler, iç denetçi yönetimle birlikte

[299] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 24.
[300] Cain, **a.g.e.,** s. 15.

hareket ederek risklerin tanımlanması ve değerlendirilmesi aşamalarında danışman görevi üstlenebilir[301].

Kurum risk yönetimi olgunluğu organizasyon genelinde düşünülebileceği gibi departman düzeyinde de ele alınabilir. Kurum risk yönetimi olgunluğu ile karşılaştırıldığında departmanların olgunluk seviyelerinin farklı olması, yürütülen faaliyetlerin ve kapsamın farklılık göstermesinden dolayı normaldir[302].

3.3. RİSK YÖNETİMİ TEMELLİ İÇ DENETİMDE PLANLAMA

Denetimin anahtar öğelerinden ilki olan planlama, büyük bir mesleki özen ve titizlikle hazırlanmalıdır. İç denetim planı; kurum yıllık iş planı, denetim stratejisi, iç denetim yönetmeliği, denetim evreni temelli hazırlanmalı ve cari yıl denetim kaynaklarının dağılımını, hedefleri ve iç denetim biriminin amaçlarını belirtmelidir. Ayrıca güvence ve danışmanlık faaliyetleri çerçevesinde verilecek hizmetler planda net olarak açıklanmalıdır[303].

Standartta yer aldığı şekliyle "İç Denetim Yöneticisi, kurumun hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen planlamayı riskleri dikkate alarak yapar"[304]. KRY sürecinden gelecek veriler, risk matrisi gibi, denetim planının risk yönetimi temelli hazırlanmasına imkân verir[305].

Geleneksel iç denetimde planlama denetçinin risk faktörlerine -denetim birimi tarafından tanımlanan denetlenebilir varlıkların içsel risklerine- dayanmaktaydı. Bu değerlendirme tamamen iç denetçi tarafından, varlıklar üzerinde sorumlulukları bulunan ve ulaşılabilen taraflarla yapılan görüşmelerden oluşmaktaydı[306].

KRY temelli denetimde ise, iç denetçi, kurum risk yönetimi olgunluğu çerçevesinde, kurum ve kurumdan ayrı birimlerin hedefleri ve stratejileri

---

[301] Buckley, **a.g.e.,** s. 32.
[302] Buckley, **a.g.e.,** s. 6.
[303] Spencer Pickett K. H., **Audit Planning: A Risk Based Approach,** John Wiley & Sons, USA, 2006, s. 140, Selim Georges and McNamee David, "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change", s. 154.
[304] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2.
[305] Sobel, **a.g.e,** s. 2.16.
[306] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 4.

doğrultusunda incelemelerini yapar[307] ve denetim planını kurum stratejik amaçlarını dikkate alarak hazırlar[308]. Ayrıca denetim planı hazırlanırken denetim komitesinin ihtiyaçları, yönetimin KRY politikaları ve iç denetim yönetmeliği dikkate alınmalıdır[309]. Bunların yanısıra hazırlanacak denetim planı kurumun denetim stratejisi ile de uyumlu olmalıdır.

Hazırlanacak olan iç denetim planının geleneksel denetim amaçlarının yanısıra bir de işletme hedeflerinin etkili bir şekilde belirlenip belirlenmediğini ve bu hedeflerin kurum içinde paylaşıma açık olup olmadığını saptamak da vardır[310].

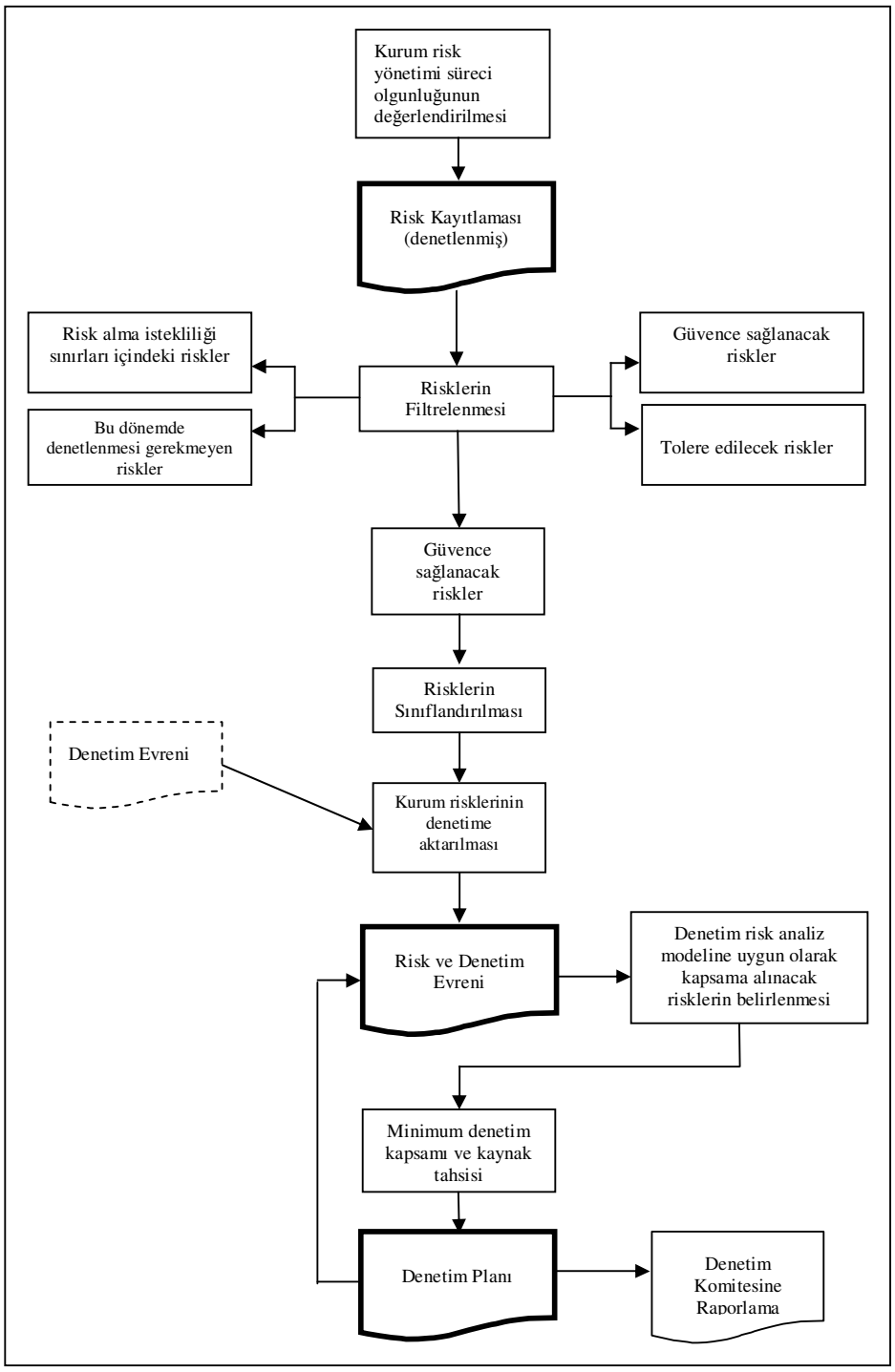
KRY temelli iç denetim faaliyetinin planlanması uygulamada genellikle aşağıdaki faaliyetleri içermektedir[311]:

- Risk yönetim sürecinden veri aktarımı,
    - Risk kayıtlaması,
    - Denetim evreninin hazırlanması,
    - İşletme risk süreçlerinden denetim programına risk transferi (risk kayıtlaması aracılığıyla),
    - Gerekli güvence seviyesinin belirlenmesi,
- Denetim planının tasarlanması,
    - Minimum denetim kapsamının belirlenmesi (üst yönetim ve denetim komitesinin istekleri doğrultusunda),
    - Denetim planının hazırlanması ve denetim komitesine raporlama,
    - Plana son şeklinin verilmesi.

İç denetimin planlama aşamalarını ifade eden faaliyetler uygulamada bazen birleştirilmektedir. İzleyen şekilde bu faaliyetlerin önemlileri akış şeması şeklinde tasarlanmıştır.

---

[307] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 11.
[308] Abela-Reid Carmen, "Risk Based Audit Planning", **The Institute of Internal Auditors-Ottawa Chapter,** 6 January 2005, s. 15.
[309] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 157.
[310] Matyjewicz and D'arcangelo, "ERM Based Auditing", s. 5.
[311] Griffiths Phil, **a.g.e.,** ss. 74-75., Griffiths David, **Risk Based Internal Auditing: An introduction,** ss.23-24., Buckley, s. 31.



Şekil 10: Risk Yönetimi Temelli İç Denetimde Planlama Safhası
Kaynak: Griffiths David, **Risk Based Internal Auditing,** www.internalaudit.biz, Version 2.0.3, 15 March 2006, s. 31'den alınarak geliştirilmiştir.

Denetim planının başarısı risk kayıtlaması ve risk ve denetim evreninin etkin belirlenmesine ve bunun sonucunda işletme risklerinin denetim evrenine doğru-tam aktarılmasına bağlıdır.

Geleneksel olarak iç denetimde planlamanın ana amacı denetim için uygun süreçleri veya alanları seçerek denetimin hatalı sonuca ulaşma riskini azaltmaktır[312]. Denetimin planlanma aşaması bu haliyle danışmanlık ve güvence hizmetlerinin birleşiminden oluşmaktadır. Bu aşamada risk yönetim sistemi hakkında güvence vermeye yönelik faaliyetler yer alabileceği gibi aynı zamanda risk yönetim çerçevesinin geliştirilmesine yönelik danışmanlık faaliyetleri de yer alabilir[313].

Bütün olarak bu sürecin sonunda hazırlanacak olan denetim planı statik bir belge olarak düşünülmemeli gerektikçe veya en azından üç ayda bir kurumun değişen ihtiyaçlarına, risklerde meydana gelen değişikliklere ve denetim faaliyeti sonuçlarına uygun olarak güncelleştirilmelidir[314].

3.3.1. Denetim Stratejisi

KRY temelli iç denetimde planlama faaliyetine kurum denetim stratejisi yön verir. Denetim stratejisi genel anlamda gerçekleştirilecek faaliyetlerin çerçevesini çizer. Bu çerçeve faaliyetlerin kim tarafından yapılacağı ve izlenecek metodoloji hakkında temel kaynaktır[315].

Denetim stratejisi, risk yönetimi değerlendirmelerine, risk, kontroller ve kurumsal yönetim alanında denetçiden beklenen destek ve danışmanlık beklentilerine, üst yönetimin iç kontrole yönelik beklentilerine ve üst yönetimin denetimde yapılması gerekli sürekli kalite iyileştirmeye yönelik beklentilerine göre şekillenir[316].

Beklentilere göre şekillenen denetim stratejisi denetim faaliyetlerine yön verir. Kurum üst yönetiminin iç denetim birimine bakış açısı, risk yönetimi açısından iç denetimin sorumluluk çerçevesi ve iç denetimin üstleneceği danışmanlık-güvence hizmetleri ve denetim faaliyetindeki odak noktası temelde kurum denetim stratejisi ve felsefesinden etkilenir.

---

[312] Matyjewicz and D'arcangelo., "Beyond Sarbanes-Oxley", s. 72.
[313] The Institute of Internal Auditors, UK & Ireland, **Audit Committee Briefing – Gaining Assurance on Risks,** The Institute of Internal Auditors, UK & Ireland, January 2006, s. 4.
[314] Selim and McNamee, "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change", s. 154.
[315] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 523.
[316] Pickett Spencer K. H., **Audit Planning: A Risk Based Approach,** s. 239.

3.3.2. Risk Yönetimi Sürecinden Veri Aktarımı

Risk yönetimi sürecinin olgunluk değerlendirmesi denetçiyi, iç denetimin risk yönetimi temelli olarak nasıl uygulanacağına ilişkin bir sonuca ulaştırır. Bu durum standartta "iç denetim faaliyetinin planı, kurumu etkileyen ve etkileyebilecek risk ve risk maruz kalma durumu hakkında bir değerlendirmeye dayanmalıdır[317]" şeklinde yer almıştır.

Planlamanın ikinci aşaması; risk yönetimi sürecinden veri aktarımı; risk kayıtlaması ve denetim evreninin hazırlanması, işletme risk süreçlerinden denetim programına risk transferi (risk kayıtlaması aracılığıyla) ve gerekli güvence seviyesinin tanımlanması faaliyetlerinden oluşmaktadır.

3.3.2.1. Risk Kayıtlaması ve Denetim Evreni

Standartta denetim planı ve riskler arasında bulunması gereken ilişki genel hatlarıyla çizilmiştir. Genel çerçeve itibariyle planlama aşamasında risk kayıtlaması, kurumun iş hayatında karşılaştığı risklerin denetim planına yansıtılmasında kullanılan ve bütün riskleri topluca gösteren bir araçtır[318].

Kurumsal risk yönetim sisteminin bir aşaması olan, risk değerleme faaliyetinin ardından kurumun amaçlarına ulaşmasını etkileyebilecek önemli riskler risk kayıtlamasına aktarılır. Risk kayıtlaması doğal olarak; kurumsal risk yönetimi sürecinde risklerin tanımlanması, risklerin değerlendirilmesi ve risk tutumunun belirlenmesi aşamalarının sonuçlarından oluşur[319].

Tablo 10: Risk Kayıtlaması

Risk	İçsel Risk		Yatıştırma ve Kontroller	Kontrol Etkinliği	Kalıntı Risk		Tavsiye Edilen Faaliyetler	Kim - Ne Zaman	Risk Sahibi
	Etki	Olasılık			Etki	Olasılık			
	Rakamsal Ölçek 1-5			Güçlü, İyi ve Zayıf	Rakamsal Ölçek 1-5				

Kaynak: Griffiths Phil, **Risk Based Auditing,** Gower Publishing, USA, 2005, s. 178 ve Chambers Andrew, **Internal Auditing,** London South Bank University, Lecture Notes, London, 2006, s. 217.

[317] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2.
[318] Pickett Spencer K. H., **Audit Planning: A Risk Based Approach,** s. 105.
[319] Pickett Spencer K. H., **Auditing The Risk Management Process,** s. 85.

Tablo 10; risk kayıtlaması; etki ve olasılık açısından içsel risklere ve bu risklere ilişkin yatıştırma ve kontrollere, kontrollere ilişkin etkinlik değerlemesine, etki ve olasılık açısından kalıntı risklere, tavsiye edilen faaliyetler ve bu faaliyetlerin kim tarafından ve ne zaman gerçekleştirileceği ayrıca risk sorumlusu-sahibine ilişkin bilgilerden oluşmaktadır.

İçsel riskler, risklere ilişkin herhangi bir kontrol önleminin alınmadığı durumda işletmenin karşılaşabileceği risklerden meydana gelir. İçsel risklere yönelik alınan birtakım kontrol önlemlerinden sonra kalan risklere ise kalıntı riskler denir. İçsel ve kalıntı riskler risk kayıtlamasına sıklıkla 5'li likert ölçeği, 1-5 arası skorlama, yardımı ile aktarılırlar.

Statik bir durumu yansıtmayan risk kayıtlaması; risklerin etki ve olasılıklarının değiştiği ve kurumun sürekli yeni risklerle karşılaştığı bir ortamın ürünüdür. Risk kayıtlamasının dinamik kalabilmesi, güncelleştirilmesi ile mümkün olabilir ve bu görev de risk kayıtlamasında risk sahibi olarak belirtilen pozisyonda çalışan personele aittir[320].

Kurumsal risk yönetimi sürecinin bir çıktısı olan risk kayıtlaması, iç denetçi tarafından önemli riskleri kapsayıp kapsamadığı ve alınan önlemlerin yeterliliği açılarından değerlendirilir. İç denetçi risk tanımlamaları, sınıflandırmaları ve diğer özellikleri kurum genelindeki uygulamalar ile tutarlılıkları açısından inceler. Belirlenen yanlış, yetersiz ve tutarsız riskler denetim raporunda belirtilir ve alınması gereken önlemler tavsiye edilir[321].

Risk kayıtlaması oluşturulduktan sonra denetim evreni hazırlanır. Denetim evreni kurum karakteristiklerinden önemli oranda etkilenir ve genellikle kurumdan kuruma farklı özellikleri ön plana çıkarabilir. Kurum stratejik planı bileşenlerini de içerebilecek olan denetim evreni, genel olarak kurumun amaçlarını yansıtır[322]. Denetim evreni risk kayıtlamasına dayanmaktadır ve iç denetim yöneticisinin sorumluluğunda hazırlanır.

Denetim evreninde yer alacak denetlenebilir faaliyetler bölge, fonksiyon, yönetim birimi, harcama kategorileri veya farklı projelere dahil olma özelliklerine

[320] Griffiths Phil, **a.g.e.,** s. 68.
[321] Matyjewicz and D'arcangelo, "ERM Based Auditing", ss. 7-13.
[322] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 153.

göre sınıflandırılabilirler[323]. Bununla beraber denetim planı için temel oluşturan denetim evreni hakkında ayrıntılı bir rehber veya standart yoktur. Uygulamada çoğunlukla iç denetim departmanlarının, denetim evrenini kurum hiyerarşisine göre belirlediği, üst yönetimin ve denetim komitesinin onayını aldığı görülmektedir[324].

Risk kayıtlamasının bir uzantısı olarak da görülebilecek olan denetim evreni doğal olarak kurumsal risk yönetim sürecinin sonuçlarından etkilenir ve aşağıdaki bilgileri içermelidir[325]:

- KRY süreci sonucunda tanımlanmış ve ölçülmüş olan riskleri,
- Risk altında bulunan kurum süreçlerini ve hedeflerini,
- Risk sorumluluklarını,
- Bir önceki denetime ve gelecek denetime ait detayları,
- Risklerin kontrolüne ilişkin detayları.

Tablo 11: Denetim Evren Modeli (İlk Adım)

Süreç Tanımı	**Risk**	**Olası Risk Sonucu**	**İçsel Risk**			**Son Denetim**		**Süreç Sahibi**	**Denetim Grubu**
			Etki	*Olasılık*	*Toplam Skor*	*Görüş*	*Tarih*		
1									
2									
3									
4									
5									
			Rakamsal Ölçek 1-5						

Kaynak: Griffiths David, **Risk Based Internal Auditing,** www.internalaudit.biz, Version 2.0.3, 15 March 2006, s. 72.

Hazırlanan denetim evreninin ilk adımında bütün riskler yer alır. Ayrıca bu risklere ait etki, olasılık ve toplam skorlar, son denetim görüşü ve tarihi ile süreçten sorumlu personelin ismi denetim evreninde yer almalıdır.

[323] Zacchea Nicholas M., "Risk-based audit target selection can increase the the probability of conducting", **The Journal of Government Financial Management,** Spring 2003, s. 23.
[324] McCuaig Bruce, "Making The Audit Universe Common Ground", **Internal Auditing,** September-October 2006, ss. 30-33.
[325] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 28., Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2, 3.

Tablo 11 ilk adım denetim evren modelinde süreç tanımı sütununda yer alan riskler beşli bir sınıflandırmaya dayanarak ikinci adım denetim evrenine aktarılırlar[326]:

1. Risk değerlemesi sonucunda yüksek skora sahip olanlar ikinci adım denetim evreninde yer alacak risklerin başlıcalarıdır,
2. Madde 1'de belirtilen risklerin haricindeki risklerden kurum risk alma istekliliği sınırları içinde olanlar ikinci adım denetim evrenine dahil edilmezler,
3. Madde 1 ve 2'de belirtilmeyen risklerden; risk alma istekliliği sınırları içinde yer almamakla birlikte tolere edilebilecek olan risklerin ikinci adım denetim evrenine dahil edilmesine kaynaklar kısıtı çerçevesinde karar verilir,
4. Önceki maddelerde açıklanmayan ilk adım evreninde geriye kalan riskler, dışarıdan güvence sağlanabilecek olanlar, doğal olarak ikinci adım denetim evreninde yer almazlar.

İkinci adım denetim evreninde riskler, süreç sahibi, denetim numarası, denetim bütçesi, denetçi ismi, durum (planlama, saha çalışması, kapsamın belirlenmesi ve tamamlanmış aşamalarından oluşur), planlanan denetim rapor tarihi, tamamlanan denetim rapor tarihi ve risk hakkında görüş başlıkları yer alır.

Tablo 12: Denetim Evren Modeli (İkinci Adım)

Risk	Süreç Sahibi	Denetim Numarası	Denetim Bütçesi (Gün)	Denetçi İsmi	Durum	Planlanan Denetim Rapor Tarihi	Tamamlanan Denetim Rapor Tarihi	Risk Hakkındaki Görüş

Kaynak: Griffiths David, **Risk Based Internal Auditing,** www.internalaudit.biz, Version 2.0.3, 15 March 2006, s. 73-76.

Gün olarak ifade edilen denetim bütçesi; ilgili denetim için bir denetçinin harcayacağı gün sayısını göstermektedir. Bu sütunun toplamı o yıl veya dönem için planlanan toplam denetim gün sayısını verir. Örneğin denetim bütçesi günlük olarak; üç denetçinin olduğu ve toplamda tatil için 60, eğitim için 15, proje çalışmaları için

[326] Griffiths David, **Risk Based Internal Auditing: Three views on implementation,** s. 20.

198 ve geçici görevlendirmeler için 48 gün ayrıldığı varsayımı altında bir yıllık mesai gün sayısı bazında aşağıdaki gibi hesaplanır[327]:

Hafta içi günler	(52x5) x 3	780
(-) Tatil	3 x 20	60
(-) Eğitim	3 x 5	15
(-) Proje Çalışması	3 x 66	198
(-) Geçici Görevlendirme	3 x 16	48
Denetime Ayrılabilir Gün		459

İlk adım denetim evren modeli, cari yıl içinde denetim imkânı olmasa bile -kapsam kısıtı, kaynak yetersizliği veya düşük önemlilik nedenlerinden dolayı- muhtemel denetim alanlarının tamamını içermelidir[328]. Bu çerçeve içinde temel işletme süreçleri, bütün önemli varlıklar, önemli uyum sorunları ve temel projeler gibi faktörler yer alır. Denetim evreni oluşturulması sürecinin en sıkıntılı kısmı evrene dahil edilecek öğelerin belirlenmesi ve bu faktörlerin önem seviyelerinin saptanmasıdır[329].

Denetim evreni oluşturulması sürecinde tartışmalı bir diğer durum da evrende yer alacak faaliyet sayısıdır. Richard Chambers tarafından yapılan araştırma sonuçlarına göre uygulamada denetim evreninin 20'den az faaliyet içerdiği durum % 4,5; 21-50 arası faaliyet içermesi % 20,8; 51-100 arası faaliyet içermesi % 21,2; 101-500 arası faaliyet içermesi % 41,7 ve 500'ün üzerinde faaliyet içermesi % 11,8 olarak belirlenmiştir[330]. Araştırma sonuçları uygulamada denetim evreninin ağırlıklı olarak 101-500 arasında faaliyeti içerdiğini ortaya koymuştur.

Denetim evreninin doğru olarak oluşturulması ve evrene dahil risklerin sıralamasının doğru yapılması denetim kaynaklarının kullanımı açısından çok önemlidir. Geleneksel iç denetimin, denetim evrenini ve evrendeki sıralamayı kısmen daha az önemli faktörlere dayandırması denetim kaynaklarının daha az önemli alanlara ayrılmasına ve denetimde odak noktanın yanlış belirlenmesine yol açmaktaydı. Bu sakıncalı durum kurumsal risk yönetimi temelli çalışan iç denetim

[327] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 75.
[328] Griffiths Phil, **a.g.e.,** ss. 73.
[329] McNamee and Selim, **Risk Management: Changing the Internal Auditor's Paradigm,** s. 49.
[330] Chambers Richard F., "Assessing Risk in Audit Planning", **European Internal Audit Conference,** 08.10.2004.

için, risk yönetimi olgunluk seviyesinin yüksek olduğu durumda, sözkonusu değildir[331].

Hazırlanan denetim evreninin güncelleştirilmesi denetim faaliyetinin etkin yürütülmesi açısından çok önemlidir. Güncelleştirme işlemi en azından yılda bir kez yapılmalı ayrıca stratejik planı ve kaynak dağılımını etkileyecek her türlü yenilik ve programların yenilenmesi gibi ayrıntılar gerekiyorsa denetim evrenine yansıtılmalıdır[332]. Bazı şartlar altında, güncel değişiklikler ve ihmal edilemez denetim sonuçları gibi, denetim evreninin daha sık güncelleştirilmesi gerektiği unutulmamalıdır[333].

Risk yönetimi temelli denetim, getirmiş olduğu farklı bakış açısına rağmen, özellikle denetim evreninin oluşturulmasına yönelik uygulama boşluğu bulunmaktadır. Denetim evreni çerçevesinin neye göre belirleneceğine ilişkin standartta herhangi bir ayrıntı olmaması uygulamada sıkıntıya neden olmaktadır. Bruce McCuaig tarafından 2006 yılında yapılan araştırmada denetim komitesi, üst yönetim ve iç denetçilerin denetim evreninin nasıl oluşturulacağına ve hangi varlıkların veya faaliyetlerin denetleneceğine veya denetlenmeyeceğine ilişkin farklı varsayımlarının bulunduğuna yönelik tespiti dikkatleri çekmektedir[334]. Standartta net açıklamanın yer almadığı ve sorumluluğun üst yönetimde bulunduğu gerçeğinden hareketle denetim evrenine nihai şeklinin verilmesi sürecinde üst yönetimin onayının alınması denetim felsefesine en uygun çözüm yoludur.

Denetim evreni ile bir anlamda denetlenecek alanlar önceliklendirilmektedir. Risk ve riske maruz kalmanın önemine bağlı olarak, mevcut kaynakların, ne şekilde tahsis edileceğine karar verebilmek için önceliklerinin belirlenmesi gerekir. Muhtemel denetim alanları arasında iç denetim yöneticisinin söz konusu öncelikleri belirlemesine yardımcı olabilecek çeşitli risk faktörleri bulunmaktadır[335].

---

[331] McCuaig Bruce, "Considering Risk in Audit Planning", **Internal Auditing,** July-August 2006, s. 12.
[332] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 154.
[333] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2, 4.
[334] McCuaig, **a.g.e.,** s. 31.
[335] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2010-2.

Bu faktörler şu şekilde sıralanabilir[336]:

- Mali etkiler (yıllık gelir ve bütçe büyüklüğü gibi),
- Varlıkların likiditesi,
- Çalışan sayısı,
- Gerçekleştirilen işlem sayısı ve hacmi,
- Yönetim ve çalışanların devir oranı ve kalitesi,
- Dış faktörlere bağlılık derecesi (ortaklar, yasal düzenlemeler gibi),
- İç kontrollerin kalitesinin değerlendirilmesi,
- Denetim görevlendirmesinin süresi,
- Son denetimin ne kadar zaman önce yapıldığı,
- Saptanan hile vakaları,
- Kurum yapısının karmaşıklığı (işlemler, teknoloji, iş hayatı),
- Merkezi bilgi sisteminin yeterliliği,
- Güvenlik önlemlerinin yeterliliği,
- Ürün geliştirme ve yeni operasyonlar,
- Onaylanmış bütçeden sapmalar,
- Muhasebe sisteminde yapılan son değişiklikler,
- Anahtar personelde yapılan son değişiklikler,
- Büyüme hızı,
- Çalışan memnuniyeti,
- Genel merkezden uzaklık.

[336] **Uluslararası İç Denetim Enstitüsü,** Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi, 2010-2, Griffiths Phil, a.g.e., s. 78, McCuaig, "Considering Risk in Audit Planning", s. 4., Koutoupis Andreas G. and Tsamis Anastasios, "Reengineering Internal Audit and Compliance Functions within Greek Banks", **Fourth European Academic Conference on Internal Audit and Corporate Governance,** City University Cass Business School, UK, 6-7 April 2006, s. 48, James M. Patton, John H. Evans and Barry L. Lewis, **A Framework for Evaluating Internal Audit Risk,** The Institute of Internal Auditor Research Foundation, 1982, s. 20.

Bireysel iç denetim uygulamalarında denetlenecek alan ve iç denetçinin tecrübesine bağlı olarak istenilen risk faktörleri kullanılabilir[337] fakat kurum genelinde yapılacak denetimler için standartta yer alan risk faktörleri arasından yönetimin görüşü doğrultusunda seçim yapılması daha sonradan ortaya çıkabilecek sorunları ve yönetimle yaşanabilecek olası çatışmaları engeller[338].

3.3.2.2. İşletme Risk Süreçlerinden Denetim Programına Risk Transferi

Risklerin denetim programına aktarılması denetim kapsamının belirlenebilmesinin temel adımıdır[339]. Bu aşamada kurum risk yönetimi sürecinin en temel çıktılarından biri olan risk kayıtlaması ve risk haritası veya matrisi aracılığıyla denetimde dikkate alınacak öncelikli alanlar belirlenir. Risklerin denetime aktarımının beklenen katkıyı gerçekleştirmesi risk yönetimi sürecinden gelecek verilerin kalitesine bağlıdır.

Risk kayıtlaması ve risk matrisi-haritasının yanısıra yönetim tarafından denetim önceliklerinin belirlenmiş olmasının etkili bir denetim planının hazırlanmasında kritik bir önemi bulunmaktadır[340].

Bu süreçte risk kayıtlaması veya denetim evreninden elde edilecek sıralanmış riskler denetimin zamanlaması, kaynakların tahsisi ve denetlenecek bölgenin (coğrafi olarak) belirlenmesi açılarından denetim programının hazırlanması ve planlama aşamalarında kullanılır[341].

Denetçi, denetim evreninin hazırlanması ile beraber sıralanan risklere ilişkin denetim yaklaşımını; güvence vermek veya danışmanlık yapmak şeklinde belirler. İki faaliyet arasındaki yönlendirme direkt olarak kurum risk yönetimi olgunluk seviyesi ile ilgilidir. Sonuç olarak danışmanlık ve güvence arasındaki tercih hakkı üst yönetime aittir ve denetçi üst yönetimin kararına uygun hareket eder.

3.3.2.3. Gerekli Güvence Seviyesinin Belirlenmesi

Denetim, genel olarak hiçbir alan için mutlak düzeyde güvence vermemekte ve mutlak doğru sonuçlara ulaşamamaktadır. Denetimden talep edilecek güvence

[337] McCuaig, "Considering Risk in Audit Planning", s. 4.
[338] Zacchea, **a.g.e.,** s. 24.
[339] Griffiths David, **Risk Based Internal Auditing: Three views on implementation,** s. 22.
[340] Griffiths Phil, **a.g.e.,** ss. 74-75.
[341] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 32.

seviyesinin düzeyi denetimin kapsamından denetime ayrılan bütçeye kadar bir dizi faktör tarafından etkilenmektedir.

Yönetim tarafından istenecek güvence seviyesi işletmenin veya faaliyette bulunulan sektörün doğal özelliklerinden etkilenebileceği gibi kurum risk alma istekliliğinden de etkilenebilir[342]. Gerekli güvence seviyesini etkileyen diğer bir faktör de kurum risk yönetimi olgunluğudur. Risk yönetiminin olgunluk seviyesi arttıkça istenecek güvence seviyesi de genelde azalmaktadır.

Güvence seviyesine bağlı olarak denetimin kapsamı ve gerekecek test miktarı değişir. Örneğin, yüksek önem derecesine sahip alanlar için istenecek güvence seviyesi doğal olarak normal önem derecesine sahip alanlardan yüksektir[343].

Güvence seviyesinin belirlenmesinde kullanılacak veriler, başta KRY'nin olay tanımlama ve risk değerleme aşamaları olmak üzere denetim planlaması öncesinde kurum yapısının anlaşılması ve risk yönetimi olgunluğunun değerlendirilmesi sonucu elde edilir.

3.3.3. Denetim Planının Tasarlanması

Denetim planın tasarlanması süreci üst yönetim ve denetim komitesinin istekleri doğrultusunda minimum denetim kapsamının ve denetim önceliklerinin belirlenmesi, denetim planının hazırlanması ve denetim komitesine raporlama yapılmasıyla birlikte plana son şeklinin verilmesi aşamalarından oluşur.

Denetim planının tasarlanması sürecinde denetçi[344];

- Denetim hedefi ile denetlenebilir birimin amacı, kurum genel amaçları ve misyonu arasında pozitif yönde bir ilişki olduğundan,
- Denetim programının denetim hedeflerine ulaşılabilmesi için gerekli kanıtları üretebileceğinden,
- Uygulanacak her testin, denetim programında denetim programı çerçevesinde istenen kanıtlara ulaştıracağından

emin olmalıdır.

[342] Buckley, **a.g.e.,** s. 35.
[343] Griffiths Phil, **a.g.e.,** s. 75.
[344] McNamee, "Risk Based Auditing", s. 26.

3.3.3.1. Denetim Kapsamının Belirlenmesi

Denetim planlanması aşamasında belirlenecek olan denetim kapsamı, genel olarak denetim faaliyetleri arasına dahil edilecek ve edilmeyecek faaliyetlerin çerçevesini çizer. Denetim kapsamı ile denetim amaçları ve öncelikleri arasında yüksek düzeyde bağlantı vardır[345].

Bununla beraber kurum hedefleri, denetlenecek faaliyetlere ilişkin önemli riskler, denetim fonksiyonlarına ayrılan kaynaklar ve kurum risk yönetimi faaliyetlerinin etkinliği[346] denetim kapsamının çerçevesini denetim evreni aracılığıyla etkiler[347]. Bu süreçte doğal olarak geçmiş yıllar denetim sonuçlarının ve üst yönetimin isteklerinin etkileri ihmal edilemez.

Kurumsal risk yönetimi özelinde belirlenecek olan denetim kapsamı aşağıda sıralanan faktörler dikkate alınarak belirlenir[348]:

- Denetimin nedeni,
- Hedefler, riskler ve ilgili aşamalar ve anahtar kontroller,
- Çalışma programı,
- Denetim süreçlerinin sınırları,
- Yönetim istekleri gibi özel durumlar,
- Denetim faaliyetini gerçekleştirecek personel ve özel sorumluluk alanları,
- Denetim zamanlaması,
- Risk yönetimi olgunluğu.

3.3.3.2. Denetim Komitesine Raporlama ve Plana Son Şeklinin Verilmesi

İç denetim yöneticisinin gözetiminde hazırlanan denetim planı üst yönetime, yönetim kuruluna ve denetim komitesine gözden geçirmeler ve onaylamalar için sunulur ve onaylamanın ardından uygulamaya konur. Eğer planda değişiklik talep edilirse iç denetim yöneticisi tarafından gerekli düzeltmeler yapıldıktan sonra plan tekrar tarafların onayına sunulmalıdır[349].

---

[345] Lawrence and others, **a.g.e.,** s. 223.
[346] De La Rosa Sean, "ERM Based Audit Reports", **Internal Auditor,** December 2005, s. 73.
[347] Abela-Reid, **a.g.e.,** s. 8.
[348] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 41.
[349] Moeller, **Brink's Modern Internal Auditing,** s. 183., Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2020-1.

Denetim planında genel olarak hangi faaliyetlerinin denetleneceği, denetimin ne zaman gerçekleştirileceği ve ne kadar süreceği, her denetimin hangi riskleri içerdiği ve bu faaliyeti gerçekleştirecek personel açıklanır[350].

Denetim planı uygulamada genellikle yıllık ve üçer aylık dönemler için tasarlanır. Yıllık plan bir yıl boyunca tamamlanacak denetim faaliyetlerini ve bu faaliyetlerin hangi çeyrekte yer alacağını gösterir. Günümüzün hızlı değişen dış ve iç çevre koşullarında yıllık planın gelişmeleri izleyememesi, yıllık planın yanısıra çeyrek dönemler için de planlama yapılma zorunluluğunu ortaya çıkarmıştır. Üçer aylık planların yıllık planlara göre ortaya çıkabilecek riskleri belirleme olasılığı daha fazladır. Çeyrek dönemlik planlar genel olarak Nisan-Haziran, Temmuz-Eylül, Ekim-Aralık ve Ocak-Mart dönemlerini kapsayacak şekilde tasarlanır[351].

Tablo 13: Yıllık Denetim Planı

Referans	Denetim	Risk Skoru	Kaynak	Denetim Tipi	Özel Faktörler	Dönem 1	Dönem 2	Dönem 3	Dönem 4

Kaynak: Spencer Pickett K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** John Wiley & Sons, USA, 2004, s. 160.

Yıllık denetim planı genelde; denetlenecek alana ait referans numarası, denetlenecek alan, risk skoru, kaynak, denetim tipi, özel faktörler ve denetimin hangi çeyrekte gerçekleştirileceği bilgilerinden oluşur.

3.3.4. Risk Yönetimi Temelli Planlamanın Yararları

Planlamanın temel faydası, plan çerçevesinde yer alan faaliyetlerin yüksek önem seviyesinde konular olduğu ve denetimde odak noktanın yakalandığına yönelik sağlanan güvencedir. Temelde, kıt denetim kaynaklarının etkin bir şekilde kullanımı -yüksek riskli alanlara aktarılması- ancak etkin bir planlama ile mümkün olacaktır[352].

Ana faydası denetim kaynaklarının yüksek riskli alanlara aktarılması olan denetim planı için sözkonusu kıt kaynak sadece parasal olarak düşünülmemelidir. Denetim faaliyetlerinin yürütülmesi sırasında zamanın etkin kullanımı ve denetimde

[350] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 34.
[351] Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 160.
[352] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 599.

zamanlılık denetimin hedeflenen sonuçlara ulaşması açısından çok önemlidir. Özellikle risk yönetimi sistemine ilişkin etkinlik denetimlerinde hatalı çalışan bir alanın belirlenmesi veya gözardı edilen bir risk tanımlamasının dikkate alınması gerekliliğinin belirlenmesi ve bu tespitlerin zamanında yapılabilmesi zamanlılık kavramını daha ön plana çıkarmaktadır.

Bunların yanısıra iyi bir denetim planı; hissedarların güvenini artırır, denetim bütçesinin etkin kullanıldığını gösterir, kurum itibarını yükseltir, iç denetçinin motivasyonunu artırır, kurum değerlerini ve hedeflerini yansıtır, düzenleyici otoritenin faaliyetlerini kolaylaştırır ayrıca bağımsız denetçinin iç denetim faaliyetinin sonuçlarına güvenini artırır bu da dolaylı olarak bağımsız denetçinin iş yükünü azaltır[353].

3.4. RİSK YÖNETİMİ TEMELLİ İÇ DENETİMİN YÜRÜTÜLMESİ

Kurumsal risk yönetiminin çıktıları sayesinde denetimde odak nokta, yüksek riskli alanlar ve sınırlı kaynakların tahsis edileceği alanlar belirlenir. Sözü edilen faaliyetler, denetimde kurum yapısının anlaşılması ve risk olgunluğu ile risk yönetimi sürecinin değerlendirilmesi aşamalarında gerçekleştirilir.

Bundan sonra sıra hazırlanan denetim planı çerçevesinde denetim faaliyetlerinin gerçekleştirilmesindedir. Denetimin etkinliği açısından planlanan faaliyetlerin belirli bir sıralamada gerçekleştirilmesi önemlidir.

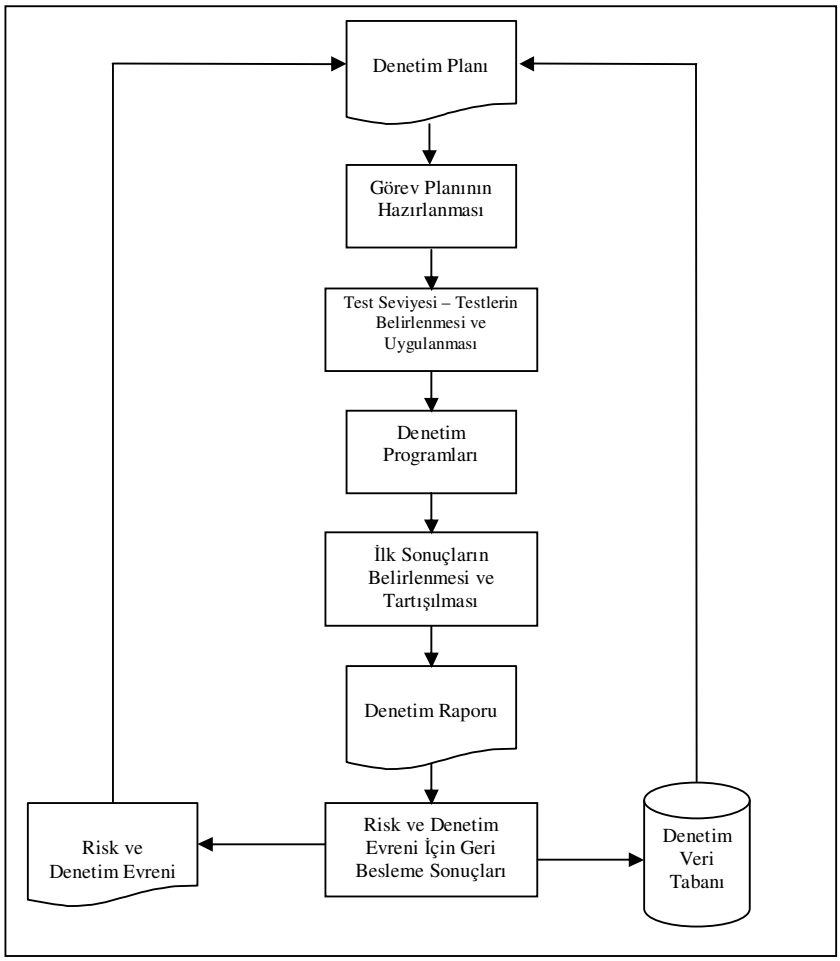
İç denetim faaliyeti genel olarak aşağıdaki sıralamada gerçekleştirilebilir[354]:

- Görev planının hazırlanması,
    - Denetim personelinin tahsisi,
    - Denetim konusunun araştırılması,
        - Geçmiş dönem denetim raporları ve çalışma kâğıtları,
        - İstatistik ve trendler,
    - Çalışma kâğıtlarının tasarlanması,
    - Kapsam ve hedefin belirlenmesi,
- Test seviyesi ve testlerin belirlenmesi ve uygulanması (inceleme mi yoksa denetim mi?),

[353] Pickett Spencer K. H., **Audit Planning: A Risk Based Approach,** s. 28.
[354] Griffiths Phil, **a.g.e.,** ss. 97-115.

- Denetim programları,
- Denetim araçları.

Yukarıda açıklanan sıralamaya paralel olarak denetimin yürütülmesi safhası biraz daha geniş perspektifte temel adımlarıyla izleyen şekilde ele alınmıştır.



Şekil 11: Denetimin Yürütülmesi Safhası

Kaynak: Griffiths David, **Risk Based Internal Auditing: An Introduction,** www.internalaudit.biz, Version 2.0.3, 15 March 2006, s. 39'dan alınarak geliştirilmiştir.

3.4.1. Görev Planının Hazırlanması

Her denetim görevi için, kapsam, amaç, zamanlama ve detaylı harcama bütçesini dikkate alan, yıllık iç denetim planı çerçevesini gözeten ve denetimin başlama ve sonlandırılma tarihini gösteren bir görev planı hazırlanır[355].

[355] Vallabhaneni Rao S., **CIA Exam Review Volume 1: Internal Audit Activity's Role in Governance, Risk and Control,** John Wiley & Sons, USA, 2005, s. 4.

Görev planının hazırlanması süreci denetim personelinin tahsisi, denetim konusunun araştırılması, çalışma kâğıtlarının tasarlanması ile denetim görev ve kontrol listelerinin hazırlanması aşamalarından oluşur.

Görev planın hazırlanması sürecinde denetim alanlarında iletişim kurulacak çalışanlar, denetimin yürütülmesi esnasında ihtiyaç duyulabilecek belgeler ve kayıtlar ve tahmini denetim süresi belirlenmelidir[356].

3.4.1.1. Denetim Personelinin Tahsisi

İç denetim yöneticisi, görevin amaçlarına ulaşmak için gereken kaynakları, para ve zaman açısından, tespit eder. Denetim personelinin tahsisi görevin niteliği, karmaşıklığı, zaman kısıtlamaları ve mevcut kaynaklar dikkate alınarak belirlenir[357]. Yukarıda ifade edilen klasik faktörlerin yanısıra KRY temelli yürütülen iç denetim faaliyetlerinde ise, KRY süreçleri arasında yer alan risk değerleme aşamasının sonuçları iç denetçilerin denetim alanlarında görevlendirilmesinde ve bireysel denetim planlarının hazırlanması aşamasında önemlidir.

Denetim amaçlarının, kapsamının ve yönteminin oluşturulması sürecinde mevcut denetim elemanlarının ve diğer kullanılabilir kaynakların çok önemli rolü vardır. Örneğin kısıtlı bir ulaşım bütçesi yerel ofis ziyaretlerini aksatabileceği gibi nitelikli eleman eksikliği de denetimin çeşitli alanlarında denetlenecek departman çalışanlarını kullanmayı veya daha az nitelikli eleman kullanmayı gerektirebilir[358].

Denetim personelinin tahsisini ve genel olarak bütçeyi ilgilendiren temel konu denetim için görevlendirilecek personel sayısıdır. Genellikle üç haftayı aşmayacak yurt içi denetimlerde deneyimli bir denetçi yeterli iken eğer sözkonusu denetim yurt dışı görevi ise iki denetçinin görevlendirilmesi tercih edilmektedir[359].

3.4.1.2. Denetim Konusunun Araştırılması

Görev planının hazırlanabilmesi için ilgili alan hakkında yeterli bilgiye sahip olmak gerekmektedir. Bu araştırmanın sorumluluğu ya denetim yönetiminde ya da o

---

[356] Griffiths Phil, **a.g.e.,** ss. 102-103.
[357] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2230-1.
[358] Vallabhaneni, **CIA Exam Review Volume 1: Internal Audit Activity's Role in Governance, Risk and Control,** s. 272.
[359] Griffiths Phil, **a.g.e.,** s. 98.

alanın denetiminde görevlendirilen sorumlu iç denetçidedir. Görevlendirilen alan hakkında bilgi; geçmiş dönem çalışma kâğıtları ve denetim raporları incelenerek, organizasyon sorumluluk şeması gözden geçirilerek ve diğer ilgili denetim materyalleri değerlendirilerek elde edilebilir[360].

İlgili alan hakkında gerekli verilere; anahtar bilgilerin, istatistiklerin ve trendlerin gözden geçirilmesi, analitik inceleme prosedürleri yardımıyla ve diğer güvence sağlayıcıların raporları aracılığıyla da ulaşılabilir[361].

Kurumsal risk yönetimi temelli denetim için denetim konusunun araştırılması; yukarıda ifade edilen klasik denetim konusu araştırmalarının yanısıra risk yönetimi aşamalarını da içermelidir. Doğal olarak sözkonusu alan hakkında yapılmış risk çalıştayları ve bu sürecin temel çıktısı olan risk haritaları denetçi için temel veridir. Genel çerçeve itibariyle bu sürece risk yönetimi olgunluk seviyesi yön verir.

3.4.1.3. Çalışma Kâğıtlarının Tasarlanması

Denetimin planlanması da dahil olmak üzere yürütülmesi safhasında ulaşılan verilerin kayıtlanması, saklanması ve ulaşılan denetim sonucunun desteklenebilmesi-açıklanabilmesi açısından çalışma kâğıtları çok önemlidir[362].

Bu ihtiyacı karşılayabilmek için çalışma kâğıtları, açık bir dille hazırlanmalı, denetim alanlarını gösterir bir dizin içermeli, denetim görüşünü desteklemeli, ve standart özellikler taşımalıdır. Ayrıca her çalışma kâğıdı denetim görevinin ismi, tarih ve denetçi ismi gibi önemli detaylara sahip olmalı, hazırlayan denetçi tarafından imzalanmalı ve mümkünse özet içermelidir[363].

Bu özelliklerin yanısıra çalışma kâğıtlarının hazırlanması sürecinde aşırıya kaçmamalı, ekonomik davranılmalı, bilgilerin kaynağı net bir şekilde ifade edilmeli ve çalışma kâğıtlarında cevabı olmayan sorular bulunmamalı eğer yer alması mutlaka gerekiyorsa cevaplanamama nedeni de yer almalıdır[364].

---

[360] Moeller, **Brink's Modern Internal Auditing,** ss. 303-305.
[361] Griffiths Phil, **a.g.e.,** s. 99.
[362] Moeller, **Brink's Modern Internal Auditing,** s. 333.
[363] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 682.
[364] Sawyer and others, **a.g.e.,** s. 381.

Uygun formatta hazırlanan çalışma kâğıtları çeşitleri bakımından denetim raporu, görevlendirme planı, denetim kontrol listesi, finansal analiz, risk analizleri, kapsam ve hedef notları, denetim kapsamı, denetim programı, kontrol hedefleri ve test programı olarak sıralanabilir[365].

Yukarıda genel olarak ifade edilen geleneksel iç denetim çalışma kâğıtlarına ek olarak iç denetimin kurum risk yönetimi sürecinde üstlendiği role ve kurum risk yönetimi olgunluğuna bağlı olarak risk tanımlamaları, risk kayıtlaması, risk haritası veya risk matrisi ve risk-denetim evreni de çalışma kâğıtları arasında yer almalıdır.

Çalışma kâğıtları, belgeleme şeklinde el ile hazırlanabileceği gibi bilgisayar ortamında da denetim yazılımları yardımıyla da hazırlanabilir. Günümüzde çalışma kâğıtları genelde bilgisayar ortamında hazırlanmaktadır. İçerik olarak her iki tür de aynı olmakla birlikte bilgisayar ortamında hazırlanan çalışma kâğıtları teknolojik faktörlerden dolayı ekstra önlemler içermelidir. Bu önlemler; çalışma kâğıtlarının yedeklenmesi, güvenliği ve çalışma kâğıtlarına erişim prosedürü[*] olarak sıralanabilir[366].

Çalışma kâğıtlarının hazırlanmasının yanısıra saklanması ve kimlerin erişimine açık olacağı da önemlidir -çalışma kâğıtlarının bilgisayar ortamında hazırlanması, dağıtımı ve saklanmasıyla beraber bu konunun önemi artmıştır- ve bu sorumluluk iç denetim yöneticisinindir. "İç denetim yöneticisi, gerektiğinde bu kayıtları kurum dışına vermeden önce üst yönetimin ve hukuk danışmanının onayını almalıdır. Ayrıca çalışma kâğıtlarına erişim ve bunların kontrolü iç denetim yönetmeliğinde ayrıntılı bir şekilde açıklanmalıdır"[367].

3.4.1.4. Kapsam - Hedeflerin Belirlenmesi ve Kontrol Listeleri

Denetimin planlanma aşamasında genel olarak kurum çapında yürütülecek denetim faaliyetlerinin kapsamı ve hedefleri belirlenmektedir. Bunun yanısıra gerçekleştirilecek her denetim görevi için de kapsam ve hedeflerin belirlenmesi gerekmektedir.

---

[365] Griffiths Phil, **a.g.e.,** s. 101.

[*] Burada açıklanmak istenen; çalışma kâğıtlarına bilgisayar ortamında erişmenin teknik ve idari (kullanma, değiştirme, onay yetkisi ve elektronik imza kullanımı gibi) bazı işlemlerin alt yapısının bilgi işlem teknolojisine uygun hazırlanmasıdır.

[366] Vallabhaneni, **CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** s. 9.

[367] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2330.A1-1.

Görev alanına ilişkin sınırların detaylı bir şekilde belirleneceği kapsamın belirlenmesi aşamasında; denetlenecek ve denetlenmeyecek alanlar, iletişim kurulacak personel, denetim süresi, zaman ve denetimi gerçekleştirecek personel ayrıntılandırılır[368]. Kapsamla birlikte göreve ilişkin denetim hedefleri saptanır. Yönetim isteklerine göre şekillenecek olan denetim hedefleri ayrıca denetim elemanlarının yeterliliklerinden, görev konusunun özelliklerinden ve göreve ayrılabilir kaynaklardan ve zamandan etkilenir[369].

Denetim kapsamının belirlenmesi kontrol listelerinin hazırlanmasıyla son bulur. Denetimin etkili bir şekilde yürütülmesini sağlayacak olan kontrol listeleri işlemlerin yürütüleceği kronolojik sıralamaya göre hazırlanırlar[370].

3.4.1.5. İç Denetim Görevlendirme Yazısı

Görev planın hazırlanması süreci tamamlandıktan sonra denetlenecek birime haber verilir. Bu yazı aracılığıyla karşı taraf denetimin zamanı, denetimin kim tarafından yapılacağı ve denetimin niçin planlandığı hakkında bilgilendirilmiş olur. Genel olarak aşağıdaki bilgiler karşı tarafa iletilmelidir[371]:

1. Adres: Denetlenecek birim yöneticisinin ismi yer alır,
2. Denetimin kapsam ve hedefi: Denetlenecek birime denetimin planlanma amacı ve kapsam açık olarak bildirilmelidir,
3. Denetimin planlanan başlangıç tarihi ve planlanmış denetim süresi: Mümkünse tarihler hakkında karşı taraf bilgilendirilir,
4. Denetimden sorumlu kişi: En azından sözkonusu denetim için denetim sorumlusu belirtilmelidir,
5. Önceden hazırlık ihtiyacı: Denetim ziyaretinden önce, denetim süresince ihtiyaç duyulabilecek her türlü materyal karşı tarafa bildirilmelidir. Bu ihtiyaçlar özel raporlar hazırlanması şeklinde olabileceği gibi çalışma alanı, bilgisayar desteği ve sisteme giriş şifreleri de olabilir.
6. Mektup örneğinin gönderildiği yerler: Mektup örneklerinin gönderildiği yönetim kademeleri mektupta yer almalıdır.

---

[368] Griffiths Phil, **a.g.e.,** s. 102.
[369] Moeller, **Brink's Modern Internal Auditing,** s. 301.
[370] Griffiths Phil, **a.g.e.,** s. 101.
[371] Moeller, **Brink's Modern Internal Auditing,** s. 306.

3.4.2. Test Seviyesi ve Testlerin Belirlenmesi ve Uygulanması

Denetimin planlama aşamasında denetim evreni sonuçlarına uygun olarak, test seviyelerinin belirlenmesinin ardından, her görev alanı için kullanılacak testler ve yöntemler belirlenir.

İlgili denetim konusunun risk seviyesine, kurum için önemlilik seviyesine ve diğer ilgili faktörlere dayanarak test seviyeleri diğer bir ifadeyle de görevlendirme kapsamı belirlenir. Test seviyesi, gözden geçirme şeklinde olabileceği gibi kapsamlı bir denetim faaliyeti şeklinde de olabilir[372].

Denetim alanları için test seviyelerinin belirlenmesi aşamasını, uygulanacak testlerin seçimi aşaması izler. Testlerin denetim görüşünü destekler kanıtlara ulaşabilmesi test amaçlarının doğru belirlenebilmesine, testlerin zamanında ve tam olarak gerçekleştirilmesine, ulaşılan sonuçların doğru yorumlanmasına ve denetim hedeflerine etkisinin doğru belirlenmesine bağlıdır[373].

Görev alanından sorumlu denetçi ve iç denetim yöneticisi tarafından uygulanacak test veya testler belirlenir. Başlıca denetim testleri analitik inceleme, görüşme, gözlem, izleme testi, anakütle denetimi, doğrulama, işlem testi ve uygunluk testi olarak sıralanabilir[374].

Testlerin ilgili alanlara, KRY bileşenlerinden risk değerlemesi sonucu elde edilen verilerin risk kayıtlamasına geçirilmesi ve bu girdiden hareketle denetim evreninde sıralanan riskli alanlara, uygulanması ve beklentilerle sonuçların karşılaştırılmasından sonra test sonuçlarına ulaşılır. İlgili sonuçlar denetim test matrisinde gösterilir ve bu matris çalışma kâğıtları arasında yer alır.

Tablo 14: Denetim Test Matrisi

Riskli Alan	Test Yaklaşımı	Test Sonuçları	Sonuç

Kaynak: Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005, s. 9.06.

[372] Griffiths Phil, **a.g.e.,** s. 105.
[373] Pickett Spencer K. H., **The Internal Auditing Handbook,** s. 663.
[374] Griffiths Phil, **a.g.e.,** s. 106.

Risk değerlemesi sürecinde belirlenen riskli alanlara uygulanan testlerin sonuçları denetim test matrisinde gösterilir. Sözkonusu matriste riskli alan, test yaklaşımı, test sonuçları ve sonuç başlıkları yer alır. Riskli alan denetlenen alanı gösterirken, test yaklaşımı sözkonusu alana uygulanan denetim testini gösterir. Denetim test sonuçları başlığı altında test sonuçları özetlenirken denetim test matrisinin son sütununda ise sonuç başlığı altında fark-boşluk analizleri yer alır. Kontrollerin riskleri kabul edilebilir seviyeye indirip indiremediğine dayanan fark analizleri mevcut sistemdeki eksikliklerin ve eksikliklere neden olan faktörlerin belirlenmesine ve sonuç olarak da eksiklikleri gidermeye yönelik alınacak önlemlerin belirlenmesine yöneliktir[375].

3.4.3. Denetim Programları

Denetim programları, benzer denetim türleri için denetim süreçlerinin tutarlı ve etkili bir şekilde yürütülmesinde kullanılırlar. Bunlar denetim süreçlerinin içerdiği aşamaları tanımlayan ve denetçi tarafından gerçekleştirilecek testleri içeren belgelerdir[376]. İç denetçiler tarafından hazırlanacak olan denetim programları kayıtlanmalı ve saklanmalı diğer bir ifadeyle çalışma kâğıtları arasında yer almalıdır[377].

Genellikle iç denetim birimleri yinelenen denetim faaliyetleri için kullandıkları standartlaştırılmış bir takım denetim programlarına sahiptirler. Fakat özel durumlar için standartlaştırılmış denetim programları işe yaramamaktadır. İşte bu tür durumlar için programların yenilenmesi ve güncellenmesi gerekir[378].

Geçmişte denetim programlarının değişikliğe uğramadan uzun yıllar boyunca kullanıldığı görülmekle birlikte günümüzde yaşanan değişimle denetim programları da esneklik kazanmıştır[379]. Özellikle denetim kapsamına riskli faaliyetlerin alınması ve risk yönetimi sistemi etkinlik denetimi denetim programlarının sürekli güncelleştirilmesi ve esnek olmaları gerekliliğini ön plana çıkarmıştır.

---

[375] Sobel, **a.g.e,** s. 9.06.
[376] Moeller, **Brink's Modern Internal Auditing,** s. 318.
[377] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2240-1.
[378] Moeller, **Brink's Modern Internal Auditing,** s. 318.
[379] Griffiths Phil, **a.g.e.,** s. 108.

3.4.4. Denetim Araçları

Denetimde etkinliği artırmak amacıyla tasarlanmış çeşitli denetim yazılımları bulunmaktadır. Genellikle Windows uygulaması altında çalışan sözkonusu yazılımlar dosya karşılaştırmalarına, trend analizlerine ve diğer spesifik denetim testlerinin yürütülmesine uygundurlar. Özel denetim yazılımlarının yanısıra bir takım temel denetim testleri MS Excel programı veya MS Excel tabanlı hazırlanan işletmelere özgü programlar aracılığıyla da gerçekleştirilebilmektedir[380].

Günümüzde risk yönetimi sistemi ile paralel çalışan denetim sistemlerine yönelik hazır yazılımlarda mevcuttur[381]. Bu tür yazılımlarda kurumsal risk yönetimi sisteminin temel adımlarına ait çıktılar ve denetim çalışma kâğıtları, örneğin risk haritası ile risk-denetim evreni, ilişkilendirilerek, denetçinin ihtiyaç duyacağı verilerin aktarılması ve paylaşımı standart hale getirilmeye çalışılmaktadır.

3.4.5. Denetim Bulguları ve Risk Yönetimi Olgunluğunun Değerlendirilmesi

Denetimin yürütülmesi aşaması denetim bulgularına ulaşılması ile sonuçlanır. Bulgu, testler sonucunda bir sorunun, problemin, boşluğun veya fırsatın denetçi tarafından tanımlanmasıdır. Bulgular, çalışma kâğıtlarında kanıtlarıyla beraber yer almalıdır. Bu aşamada son olarak elde edilen bulgular yönetimle gözden geçirilmelidir. Bulguların yönetimle gözden geçirilmesi, olası yanlış yorumlamaları önleyecek ve riskler çerçevesinde sonuçlara son halinin verilmesine yardımcı olacaktır[382].

Denetim bulgularının özetlenmesinden ve raporlama aşamasından önce denetçi incelenen alana ilişkin risk yönetimi yapısını değerlendirmelidir. Risk yönetimi yapısı strateji, süreç, insan, teknoloji ve bilgi olmak üzere beş farklı açıdan değerlendirilir. Bu değerlendirme denetçiye denetim bulgularını risk yönetimi yeterlilikleri, muhtemel çözümler ve ek fırsatlardan yararlanma çerçevesinde değerlendirmesine imkân verir[383].

---

[380] http://www.informationactive.com, 12.03.2007.
[381] http://www.darcangelosoftwareservices.com/erm_based_auditing.htm, 19.09.2007.
[382] Sobel, **a.g.e,** s. 11.05.
[383] Sobel, **a.g.e,** s. 10.02.

3.5. RİSK YÖNETİMİ TEMELLİ İÇ DENETİMDE RAPORLAMA

İç denetim yöneticisi, iç denetim faaliyetinin amacı, yetkileri, görev ve sorumlulukları ve plana kıyasla performansı konularında, denetim komitesi, yönetim kurulu ve üst yönetime dönemsel raporlar sunar[384].

Hazırlanacak denetim raporun içeriği iç denetim biriminin yönetmeliğinden, raporlama beklentilerinden ve raporla ilgilenenlerin ihtiyaçlarından ayrıca kurum kültüründen etkilenir[385]. Bu raporlar, önemli riskleri, kontrol sorunlarını, kurumsal yönetim sorunlarını ayrıca denetim komitesi, yönetim kurulu ve üst yönetimin ihtiyaç duyabileceği veya talep edebileceği başka konuları da içerebilir[386].

İç denetim raporu, gerçekleştirilen denetim faaliyetinin amacını, kapsamını ve sonuçlarını özetler. Raporda risk, kontrol ve kurumsal yönetim sorunlarına ilişkin uyarılar yer almalı ve rapor, denetim elemanlarının performans değerlendirmelerine imkân verilmelidir. Performans değerlendirmelerinden hareketle de iç denetim elemanlarının eğitimleri ve kendilerini geliştirmelerinin yolu açılacaktır[387].

Risk yönetimi temelli denetimle birlikte, denetim sonuçlarının riskler ön planda tutularak özetlenmesi ve ilgili taraflara sunulması raporlama kalitesini artırmıştır. Bu durum geleneksel denetimde raporlamanın temelini oluşturan denetim bulgularının ayrıntılı olarak açıklandığı durumun çok ötesinde bir yaklaşımdır[388].

3.5.1. Raporlama Hedefleri ve Rapor Özellikleri

İç denetim raporunun temel hedefleri bulguların açıklanması, iç denetim fonksiyonlarının aksayan ve zayıf yönlerinin tanımlanması, tavsiyeler ve denetçi görüşünün belgelenmesi olarak sıralanabilir[389]. Bunların yanısıra raporda ayrıca risk yönetimi ve kontrollerin geliştirilmelerine ve risk-kontrol dengesine ilişkin tavsiyeler de yer almalıdır[390].

---

[384] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2060-1.
[385] Sobel, **a.g.e,** s. 11.02.
[386] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2060-1.
[387] Ratliff Richard L., Wallace Wanda A., Sumners Glenn E., McFarland William G. and Loebbecke James K., **Internal Auditing Principles and Techniques,** The Institute of Internal Auditors, USA, 2006, ss. 394-395.
[388] De La Rosa, **a.g.e.,** s. 73.
[389] Moeller, **Brink's Modern Internal Auditing,** s. 404.
[390] Griffiths Phil, **a.g.e.,** s. 117.

Denetim raporunun sözkonusu hedeflere ulaşabilmesi ve raporlama yapılan tarafların raporu gerektiği şekliyle kullanabilmesi iyi hazırlanmış bir raporla mümkün olacaktır.

İyi hazırlanmış bir rapor her şeyden önce istenilen zamanda taraflara sunulmalıdır. Zamanında taraflara sunulamayan rapor etkinliğini kaybedecek ve sorunların çözümü gecikecektir. Rapor aynı zamanda önemli alanlara odaklanmış, doğru, kısa ve öz, okuyanlar tarafından takip etmesi kolay olacak şekilde akıcı, sonucun net olarak ifade edildiği ve pratik tavsiyeleri içeren bir tarz ve üslup ile hazırlanmış olmalıdır. Ayrıca rapor; içindekiler sayfası, yönetici özeti ve eylem planını da içermelidir[391].

Yönetici özeti, yöneticilerin zamanlarının kısa olmasından dolayı raporun tümünü okuyamamaları ihtimaline karşı hazırlanmaktadır. Önemli denetim sonuçlarının vurgulu bir şekilde ele alındığı, kısa, genellikle bir sayfa hazırlanan yönetici özetinde sorunlardan ziyade çözüm yolları üzerinde durulur ve alınan önlemler özetlenir[392].

Kurumsal risk yönetimi temelli denetimle birlikte yönetici özetlerinin tamamının neredeyse risk yönetimi faaliyetlerinin etkinliğine odaklanması gerektiği tavsiye edilmektedir. Risk yönetimi etkinliği güçlü etkinlikte, orta etkinlikte ve zayıf etkinlikte risk yönetimi olarak ifade edilebilir. Rapor özetinde; kısaca belirlenen risklerin kabul edilebilir seviyeye nasıl indirilebileceği ve tek cümle ile yönetime tavsiyeler yer almalıdır. İfade edilen bu değerlendirme izleyen tabloda gösterildiği gibi bütün riskleri kapsayacak şekilde tasarlanabilir. Ayrıntılı raporda ise bu tabloda topluca gösterilen riskler ayrı ayrı ele alınarak mevcut risk yönetim uygulamalarına ve tavsiyelere yer verilir[393].

[391] Griffiths Phil, **a.g.e.,** s. 119., Pickett Spencer K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** s. 227.
[392] Griffiths Phil, **a.g.e.,** s. 137.
[393] Sobel, **a.g.e,** s. 11.09.

Tablo 15: Risk Değerlendirmeleri

		Risk Yönetimi Etkinliği		
		Güçlü	Orta	Zayıf
Risk Önemliliği	Yüksek			
	Orta			
	Düşük			

Kaynak: Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005, s. 11.10.

Denetim raporunda bulunması gereken eylem planında, sorunlu alanlar ve bu alanlardan sorumlu personel ve zamanlamaya ilişkin bilgiler yer almalıdır. Eylem planı ile riskli alanlar ve bu alanlara ilişkin gözlemlerin yanısıra iş riskleri ve organizasyona etkilerine ilişkin bilgilendirme yapılır. Ayrıca eylemlere ilişkin sorumluların belirlenmiş olması izleme sürecini kolaylaştırır.

Raporlamada dikkat edilmesi gereken bir diğer önemli konu da iç denetim raporunun dil ve format bakımından risk yönetimi raporlaması ile uyumluluk göstermesi gerekliliğidir. Her iç denetim görevlendirmesinin sonucu risk kayıtlamasının yönetim tarafından gözden geçirilmesi ve değiştirilmesini veya risk olgunluğuna ilişkin iç denetim birimi tarafından değerlendirmenin yine iç denetim tarafından gözden geçirilmesini gerektirebilir[394].

İç denetim raporu amaçlar, kapsam ile sonuç ve kanaatler kısımlarından oluşur. Amaçlar başlığında görevin hedefleri ve denetim raporunun neleri başardığı açıklanmalıdır[395].

Kapsam başlığı altında denetlenen faaliyetler ve denetlenen zaman dilimine ilişkin bilgiler yer alır[396]. Bu başlık altında ayrıca denetim evreni ve denetlenen faaliyetler arasındaki ilişki açıklanmalı, kurumun coğrafi olarak denetlenen birimleri ve denetim kanılarına ulaşmak için kullanılan teknikler ve güvenilirliklerinden bahsedilmelidir[397].

---

[394] The Institute of Internal Auditors, UK & Ireland, **Audit Committee Briefing - Gaining Assurance on Risks,** s. 4.
[395] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2410-1.
[396] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2410-1.
[397] Vallabhaneni, **CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** s. 12.

Son olarak rapor, iç denetçinin denetleme konusu faaliyetlere ilişkin tespit ve tavsiyelerini içeren sonuç ve kanaatler ile son bulur[398]. Denetçi sonuç bölümünde denetlenen faaliyetlere ilişkin profesyonel yargısını açıklar. Ayrıca sonuç bölümünde denetim bulgularından hareketle denetlenen alanlara ilişkin tavsiyelerde bulunulur[399].

Tavsiyeler yanlış anlaşılmalara fırsat vermeyecek bir biçimde net olarak ifade edilmeli ve önerilen eylemler, maliyet ve diğer açılardan uygulanabilir olmalıdır. Denetçi ve süreç sahibinin sözkonusu alanla ilgili ilerlemeyi izleyebilmesi için eylemler ayrıca ölçülebilir olmalıdır[400].

3.5.2. Üçer Aylık Raporlar ve Nihai Rapor

Raporlama genellikle üçer aylık dönemlerde ve yıl sonlarında yapılmaktadır. Üçer aylık raporlamaya daha çok erken bilgiye gerek duyulduğunda başvurulmaktadır. Ancak bu raporlar nihai raporun hazırlanması gerekliliğini ortadan kaldırmamaktadır[401].

Üç ayda bir yapılan raporlamanın avantajları; dönem sonu rapor hazırlama süresini kısaltması, acil ele alınması gereken bilgileri iletişime sunması ve resmi olmayan ve sözel formatta olmasıdır. Öte yandan resmi ve yazılı bir ara dönem raporunun dezavantajları olarak; kesin durumlara ilişkin dönem sonu raporuna ilişkin ihtiyacı ortadan kaldırması ve kanıtların tamamlanmış olma zorunluluğunun denetçiyi zor durumda bırakması sayılabilir[402].

Ortalama olarak, denetim faaliyetlerinin tamamlanmasını ve üst yönetimle hedeflenen ve ulaşılan bulguların tartışılmasını izleyen 7-10 gün içinde iç denetim yöneticisi tarafından taslak rapor, yıllık rapor öncesi, hazırlanır[403]. Taslak rapor zorunlu olmamakla birlikte uygulamada tercih edilmektedir. Hazırlanan taslak rapor ilgili yılda denetlenen alanlardan direkt sorumlu yöneticilere gönderilir.

---

[398] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2410-1.
[399] Vallabhaneni, **CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** s. 15.
[400] Sobel, **a.g.e,** s. 11.05.
[401] Sawyer and others, **a.g.e.,** s. 698.
[402] Vallabhaneni, **CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** s. 11.
[403] Griffiths Phil, **a.g.e.,** s. 122.

Yöneticilerden gelen geri bildirimlere uygun olarak denetlenen alana ilişkin alınması gereken düzeltici önlemler gözden geçirilir ve nihai rapor hazırlanır[404].

Taslak rapor tamamıyla iç denetim yöneticisinin kontrolü altındayken nihai rapor taslak rapora yönelik yorumlar çerçevesinde; üst yönetim ve denetim komitesiyle yapılan görüşmeler ile uzlaşmalar doğrultusunda hazırlanır. İç denetim birimi tarafından hazırlanan cari yıl nihai raporunda ele alınan sorunlar bir önceki yıl denetim raporunda ele alınan sorunlarla benzerlik taşıyorsa, bu durum üst yönetimin gerekli önlemleri alma konusunda iç denetim yöneticisi tarafından ikna edilemediğini gösterir. Özellikle fiziksel denetim (örneğin fabrika denetimi) için hazırlanan raporda fotoğraf veya grafik kullanılması ile denetçinin üst yönetimi ikna etmesi kolaylaşacaktır[405].

3.5.3. Raporlama Yapılacak Taraflar

İç denetim yöneticisi tarafından hazırlanan raporlar denetim komitesi, yönetim kurulu ve üst yönetime dönemsel olarak raporlar sunulur[406]. Öte yandan hazırlanan raporlar kurum içi ilgililer -üst yönetim ve diğer çalışanlar dahil- tarafından kullanıldığı gibi kurum dışı ilgililer -düzenleyici otoriteler, genel anlamda devlet ve yatırımcılar- tarafından da kullanılmaktadır.

Bu açıdan hazırlanacak raporların farklı grupların farklı ihtiyaç ve ilgilerini karşılayacak şekilde ortak bir terminoloji ve bulgulara ilişkin azami bir önem seviyesi gözetilerek hazırlanmalıdır[407].

3.5.4. Raporlama Sonrası Takip

İç denetim yöneticisi, yönetimin aldığı tedbirlerin etkili bir şekilde uygulanmasını veya üst yönetimin, gerekli tedbiri almamasının riskini üstlenmeyi kabul etmesini sağlamak ve gelişmeleri gözlemlemek amacına yönelik bir takip süreci kurmalıdır[408].

---

[404] Moeller, **Brink's Modern Internal Auditing,** s. 422.
[405] Griffiths Phil, **a.g.e.,** s. 123.
[406] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2060-1.
[407] Moeller, **Brink's Modern Internal Auditing,** s. 406.
[408] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2500.A1-1.

Takip süreci, tavsiye edilen eylemlerin uygulanıp uygulanmadığını belirleme açısından çok önemlidir. Kurum iç denetim yönetmeliğinde takip sürecinin kim tarafından ve nasıl yapılacağına ilişkin ayrıntılar bulunabilir veya iç denetim yöneticisi tarafından belirlenebilir. Genellikle takip süreci, süreç sahibi tarafından veya denetçi tarafından takip süreci denetimi veya yine denetçi tarafından odaklanılmış takip süreci incelemesi olarak gerçekleştirilebilir[409].

Denetim raporunda yer alan bulgularla ilgili güncelleştirmelerin süreç sahibi tarafından denetçiye sunulduğu takip süreci, denetçinin yeterli zamanının olmadığı durumlarda tercih edilmektedir ve bu tür bir raporlamaya objektiflik kısıtı nedeniyle güven düşük seviyededir. Ayrıca raporlama sıklığının artmasına paralel olarak raporlama bürokratik işlem olarak görülmeye başlar ve raporlama etkinliği azalır. Denetçi tarafından takip sürecinin üstlenilmesi ise denetim raporundan belli bir süre sonra tavsiye edilen eylemlerin uygulamada nasıl çalıştığının gözlenmesi ve gerekli denetim testlerinin yeniden yapılması faaliyetlerini içerir[410].

Yönetimin görevi ve sorumluluğu, görevle ilgili önemli tespit ve tavsiyeler dikkate alınarak alınması gereken tedbirler hakkında kararlar almaktır. Üst yönetim maliyetinden veya başka hususlardan dolayı, rapor edilen bir sorunu düzeltmeme veya çözmeme riskini üstlenmeye karar verebilir. Takip süreci sonunda, üst yönetimin önemli tespit ve tavsiyelere ilişkin bütün kararları, denetim komitesi ve yönetim kuruluna bildirilmelidir[411].

3.6. RİSK YÖNETİMİ TEMELLİ DENETİMİN AVANTAJ VE DEZAVANTAJLARI

Risk yönetimi temelli iç denetimin uygulandığı bir işletmede iç denetim birimi klasik denetim güvence fonksiyonlarına ilave olarak yönetim kuruluna; risk yönetimi özelinde, risk yönetimi sisteminin; riskleri kurum risk alma istekliliğine uygun olarak yönetip yönetemediğine ilişkin güvence verir[412].

---

[409] Sobel, **a.g.e,** s. 12.02.
[410] Sobel, **a.g.e,** ss. 12.04-05.
[411] Uluslararası İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** 2060-1:3.
[412] Cain, **a.g.e.,** s. 5.

Risk yönetimi temelli denetimin avantajları şu şekilde sıralanabilir[413]:

a) Risk yönetimi temelli denetim; geleneksel iç denetime göre daha zor ve karmaşık olmakla birlikte, yerleşik bir risk yönetimi sistemine sahip kurumlarda kolay uygulanabilir bir sistem olarak kabul edilmektedir.

Sistem uygulamada bütün kurumu kapsadığı için, riskler açısından, iç denetim sistemine dahil olan olmayan ayrımı ortadan kalkmakta, bu özelliği nedeniyle de bir karışıklığı önlemektedir.

b) Kaynakların doğru ve etkin kullanılmasına imkân verir. Bu da temel olarak denetim planının, denetim komitesi tarafından verilen risk güvenceleri doğrultusunda yapılacak risk değerlemeleri sonucu hazırlanmasının bir sonucudur.

Bunların yanısıra iç denetim sisteminin COSO KRY sistemi çerçevesine uygun olarak yapılandırıldığı kurumlarda uygulamada standartlaşmaya izin vermesi ve bu özelliği dolayısıyla sorunlu alanlara müdahalede dışarıdan uzman kullanımına imkân vermesi sistemin diğer bir avantajı olarak ön plana çıkmaktadır.

Ayrıca, kurum risk yönetimi olgunluk seviyesine bağlı olarak iç denetimin risk yönetim sürecindeki etkinliği, organizasyon içinde iç denetim biriminin itibarının artmasını sağlar[414].

Risk yönetimi sistemi ile bütünleştirilmiş bir iç denetim birimi riske neden olabilecek problemli alanları-olayları erken safhalarda teşhis edebilecek ayrıca risklere ve kontrollere ilişkin hedeflere ulaşabilmesi genel anlamda da işletmenin hedeflerine ulaşabilmesi için gerekli bilgileri zamanında taraflara sunabilecektir.

Risk yönetimi temelli denetimin dezavantajları ise aşağıdaki gibi sıralanabilir[415]:

a) Kurumla yakın ilişkide olunması, özellikle danışmanlık ve güvence hizmetleri arasındaki hassas dengenin varlığı iç denetimin bağımsızlığını zedeleyebilmektedir.

---

[413] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 53.
[414] Cain, **a.g.s.,** s. 31., Beasley Mark S., Clune Richard and Hermanson Dana R., "ERM A Status Report", s. 71.
[415] Griffiths David, **Risk Based Internal Auditing: An introduction,** s. 54.

İç denetim yönetimin bir parçası olduğu halde, fonksiyonel anlamda bağımsızlığa sahip bir mekanizma olarak faaliyette bulunmakta ve bu nedenle kurum ve kuruluşlarda yönetsel hesap verilebilirlik müessesesinin yerleştirilmesine çok büyük katkı sağlamaktadır[416]. KRY temelli çalışan denetim sistemi risk yönetimi sistemine bağımlılığı artıracağı ve yönetimle ilişkileri daha geniş bir tabana yayacağı için bağımsızlığı zedeleyebilir.

b) Daha önce risklerin tanımlanması, riskli faaliyetlerin ölçülmesi ve izlenmesi gibi faaliyetlerle tanışmamış kurumlar açısından risk yönetimi temelli denetimin uygulanması bir hayli sıkıntılı olabilmektedir.

İşletmenin risklere ve risk yönetimine ilişkin daha önceden kurumsal bir hazırlığının bulunmaması ilk uygulamanın hem daha fazla maliyetli olmasına yol açmakta hem de olası bir yanlışlığın telafisini imkânsız hale getirmektedir. Bu tarz sorunlar dışarıdan bağımsız uzman kullanımı ile en aza indirilebilmektedir.

c) Mevcut denetim elemanlarının yeniden eğitimi gerekebilir.

Bunların yanısıra kurumsal risk yönetimi olgunluğunun yüksek seviyede olduğu ve buna bağlı olarak iç denetimin kurum tarafından üretilen bilgi ve analizleri kullanması kurum risk yönetim sistemine yüksek düzeyde bir bağımlılığa neden olmaktadır[417]. Bu durum iç denetim biriminin risk yönetimi sistemine ve elemanlarına bağımlılığını artırmakta ve denetim temel fonksiyonu olan bağımsızlık ve güvence verme açısından olası sorunlu alan olmaktadır.

[416] Uzun Ali Kamil, "Aile İşletmelerinde Kurumsal Yönetim ve İç Denetimin Rolü", **Dünya Gazetesi,** 20.072006.
[417] Özsoy Mehmet Tahir, "Risk Odaklı Denetim, ABD Uygulaması ve Türkiye Uygulaması Açısından Değerlendirilmesi", **Active,** Mart-Nisan, 2004, s. 4.

IV. BÖLÜM
RAPOR İNCELEMELERİ, RİSK YÖNETİMİ TEMELLİ İÇ DENETİM İMKB ANKET UYGULAMASI VE MÜLAKAT ÇALIŞMASI

COSO KRY çerçevesi; risklerin bir bütün olarak değerlendirilmesi, ilgili önlemlerin kurumun bütünü dikkate alınarak belirlenmesi ve uygulamaya konması gerekliliğini vurgulamaktadır. Kullanılacak kriterler veya çerçeveler konusunda bir zorunluluk kısmen bulunmakla birlikte genel olarak risk yönetimi temelli denetim, bankalarda BASEL prensipleri ve risk sınıflandırmalarına göre yürütülmektedir. Öte yandan reel sektör işletmelerinde ise, COSO KRY çerçevesi dikkate alınmaktadır.

COSO ve BASEL ilkeleri genellikle birbirlerine paralel olmakla birlikte ayrıldıkları nokta risklerin sınıflandırılması ve ölçümüdür. Bu durum sektörlerin değişen ihtiyaçlarından, uzmanlaşma imkânlarından ve kullanılabilecek veri kalitesinden dolayı farklılaşmaktadır.

Denetimin temelinde risklerin kontrol yöntemleri ile saptanması, önlenmesi ve ortadan kaldırılması bulunduğu gerçeğinden hareketle risk yönetimi ve denetim sistemlerinin birleştirilmesinin işletmelerin kıt olan kaynaklarının kullanımının etkinliğini artıracağı açıktır.

1990'lı yılların sonuna doğru çalışmaların yoğunlaştığı bu alanda, 2004 yılında COSO KRY çerçevesinin özet olarak 2006 yılında da kapsamlı bir biçimde yayınlanması, risk yönetimi ve denetimin bağlantı noktalarının neler olacağı sorusunu cevaplanabilir hale getirmiştir.

Uluslararası iç denetim standartlarında yer alan yönlendirmeler, COSO KRY çerçevesi ve BASEL II prensiplerinin de katkılarıyla global anlamda kabul gören risk yönetimi temelli iç denetim son olarak Enron sonrası süreçte kabul edilen Sarbanes-Oxley ile birlikte Amerika'da yasal zemine kavuşmuştur. Türkiye'de ise 2006 yılında kabul edilen Bankacılık Kanunu'nda açık olarak ifade edilmese de 1 Kasım 2006'da yayınlanan "Bankaların İç Sistemleri Hakkında Yönetmelik"te, iç

denetim sisteminin amacı "iç kontrol ve risk yönetimi sistemlerinin etkinliği ve yeterliliği hakkında güvence sağlamak[418]" şeklinde ifade edilerek iç denetimin risk yönetimi üzerindeki sorumluluğunun bulunduğu gerçeği kabul görmüştür.

Global ölçekte kabul gören bu yaklaşım; iç denetimin risk yönetimi sisteminin kurulması, etkin bir şekilde işletilmesi ve etkinliğinin denetlenmesi hususunda kurumların risk yönetimi olgunluk seviyelerine paralel olarak öncü veya danışman bir rol üstlenmesi gerektiği yönündedir.

Bu çerçevede Avrupa Birliği ile uyum görüşmelerini yürüten ve BASEL II prensiplerini yakın bir gelecekte uygulamaya başlamayı planlayan bir aday ülkenin, iç denetim uygulamalarını risk yönetimi sistemi ile bütünleştirilerek bu sayede sermaye yeterliliklerinin daha sağlıklı belirlendiği, işletmelerin kıt kaynaklarının korunduğu ve etkin kullanıldığı bir ortamda olası krizlerden daha az etkileneceği ve göreceli olarak daha istikrarlı bir ekonomide ve daha etkin bir şekilde faaliyet göstereceği açıktır.

Çalışmanın uygulama safhası, faaliyet ve kurumsal yönetim uyumluluk raporları incelemesi, anket çalışması ve mülakat şeklinde tasarlanmıştır. Bu çerçevede öncelikli olarak İMKB'de faaliyet gösteren şirketlerin yıllık faaliyet raporları ve kurumsal yönetim uyumluluk raporları incelenmiştir. Ardından yukarıda sözü edilen amaca ulaşabilmek ve genel olarak Türkiye iç denetim kültürü ve uygulamalarını belirginleştirmek için anket soruları aracılığıyla değerlendirme yapılmıştır. Son olarak da KRY temelli iç denetimin Türkiye uygulaması hakkında bilgi almak, uluslararası uygulamanın uzağında kalan alanlara çözüm önerileri getirmek, risk yönetim sistemi ve iç denetimin bağlantı noktalarını ve bilgi akış süreçlerini açıklığa kavuşturmak için mülakatlar yapılmıştır.

4.1. KRY TEMELLİ İÇ DENETİME İLİŞKİN LİTERATÜR

Risk yönetimi uzun yıllardır bilim adamlarının ilgisini çekmekle birlikte risk odaklı denetim ilk olarak 1997 yılında Mcnamee tarafından yapılan "Risk Based Auditing" (Internal Auditor) isimli çalışmada incelenmiştir. Çalışmada, denetimin temelinde kontrollerin bulunduğu göz önüne alındığında risk yönetimi ve denetimin;

[418] Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankaların İç Sistemleri Hakkında Yönetmelik",** Madde 21.

kurumun hedeflerine ulaştırılması ortak paydasında buluşmaları gerektiği vurgulanmaktadır.

1998 yılında Mcnamee ve Georges tarafından yapılan ve "Changing Paradigm" (Mc^2 Management Consulting) olarak adlandırılan çalışmada geleneksel denetimden risk odaklı denetime uzanan süreç ele alınmış ve bir öngörü olarak da risk yönetimi temeli denetim irdelenmiştir.

Yine aynı yazarlar tarafından The Institute of Internal Auditors için 1999 yılında yapılan ve "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change?" (International Journal of Auditing) ve "The Risk Management and Internal Auditing Relationship: Developing and Validating Model" (International Journal of Auditing) başlıklarını taşıyan çalışmalarda risk yönetimi ve iç denetim için tanımlayıcı bir model geliştirilmiş ve ortak çalışma alanları tanımlanmış ayrıca organizasyon genelinde sistemin etkin çalışabilmesi için bilgi akışı ve ortak faaliyetler ayrıntılı olarak tasarlanmıştır. Bu çalışmanın birinci bölümünde "Bütünleştirilmiş Risk Yönetimi ve İç Denetim" başlığı altında, sözü edilen yazarların tasarladıkları model Enron sonrası süreçte denetimde yaşanan gelişmeler dikkate alınıp geliştirilerek ele alınmıştır.

2003 yılında İtalyan araştırmacılar Allegrini ve D'onza tarafından yapılan ve "Internal Auditing an Risk Assessment in Large Italian Companies: an Emprical Survey" (International Journal of Auditing) başlığını taşıyan bir çalışma yayınlanmıştır. Bu çalışmada 100 büyük İtalyan firması üzerinde bir anket uygulaması yapılmış ve iç denetim biriminin bulunup bulunmadığı, denetim planlarının risk odaklı yapılıp yapılmadığı, Kontrol Risk Öz Değerleme uygulamalarına ne ölçüde yer verildiği ele alınmıştır.

Ulusal ölçekte yapılan uygulamalı çalışmaların yanısıra 2005 yılında Beasley, Clune ve Hermanson tarafından uluslararası düzeyde; Amerika, Kanada, Birleşik Krallık ve Avustralya'yı kapsayan uygulamalı bir araştırma yürütülmüş ve araştırma süreci sonunda "ERM a status report" (Internal Auditing) isimli bir yayın yapılmıştır. Çalışmada ankete katılan işletmelerde KRY sürecinin hangi aşamada olduğu, KRY sürecinde iç denetim biriminin hangi faaliyetleri yürüttüğü ve KRY faaliyetlerinin iç denetim faaliyetlerini nasıl etkilediği ölçülmeye çalışılmıştır. Araştırmada cevaplayıcı kurumların % 48'inde KRY sürecinin ya tamamıyla faal olduğu ya da

sürecin kısmen uygulamada olduğu sonucuna ulaşılmıştır. Ayrıca iç denetim birimlerinin, orta düzeyde KRY faaliyetlerini koordine ettiği, risk tanımlama faaliyetlerine katıldığı, KRY sürecini izlediği, organizasyon içinde KRY eğitimleri yürüttüğü, sürece öncülük ettiği ve son olarak da risk değerleme çalışmalarını yürüttüğü sonucuna ulaşılmıştır.

2003 yılında yapılan İtalya örneğine benzer diğer bir çalışma da 2006 yılında Avustralya'da borsada faaliyet gösteren şirketler üzerinde Stewart ve Kent tarafından yapılan "The use of internal audit by Australian companies" (Managerial Auditing Journal) başlıklı çalışmadır. Çalışma, iç denetim ve risk yönetimi sistemleri arasındaki ilişkiyi belirlemeye yöneliktir. Çalışmada, iç denetim birimine sahip şirketlerin toplam şirketlerin üçte birini oluşturduğu ve iç denetim ile risk yönetimi sistemi arasında yüksek düzeyde bir ilişki olduğu belirlenmiştir.

2006 yılında Gramling ve Myers tarafından yapılan ve "Internal Auditing's Role in ERM" (Internal Auditor, 2006) başlığını taşıyan çalışmada; KRY sürecinde iç denetim biriminin üstlenebileceği roller ve sorumluluk alanları yapılan anket uygulaması ışığında değerlendirilmiştir. Çalışmanın sonuçları, Birleşik Krallık İç Denetim Enstitüsü tarafından yayınlanan KRY sürecinde iç denetimin temel görevleri, şartlı olarak üstlenilebilecek görevler ve üstlenilmemesi gereken görevler şeklinde ele alınan sınıflandırmaya paraleldir.

Günümüzde risk yönetim sürecine iç denetim biriminin yön verdiği ve bu süreçte ağırlığının fazla olduğunu vurgulayan ve denetim komitesinin de risk yönetiminde daha fazla etkin hale geldiği sonucuna ulaşan başka bir çalışma da Fraser ve Henry tarafından 2007 yılında yapılan "Embedding risk management: structures and approaches"dır (Managerial Auditing Journal). Çalışmada genel olarak "KRY sürecinde iç denetimin ve denetim komitesinin rolü nedir?" ve "Kritik risklerin tanımlanması sürecinde nasıl bir mekanizma mevcuttur?" sorularına cevap aranmıştır.

Anılması gereken bir diğer çalışma da Pricewaterhouse Coopers denetim ve danışmalık firması tarafından 2007 yılında yaptırılan piyasa araştırmasına dayanan "Internal Audit 2012" isimli rapordur. Çalışmada, 20. yüzyıl iç denetim planlarının kontrol güvencesi odaklı, günümüz iç denetim planlarının ise risk odaklı çalıştığı vurgulanmaktadır. Ayrıca çalışmada yakın gelecekte, Amerika'da 2012'ye kadar

KRY temelli iç denetim aşamasının tamamlanacağı tahmin edilmiş ve iç denetim sistemlerinin risk yönetimi sisteminin etkinliği hakkında güvence vermeye yönelik çalışacağına genel olarak da risk yönetimi temelli iç denetimin kullanımının yaygınlaşacağına ilişkin bir öngörüde bulunulmuştur.

Uluslararası literatürde yer alan bir diğer önemli çalışmada Collier, Berry ve Burke tarafından 2007 yılında yapılan "Risk and Management Accounting" isimli çalışmadır. Çalışma anket ve mülakat uygulaması şeklinde tasarlanmış ve "Risk yönetiminde yönetim muhasebecisinin rolü nedir ve ne olabilir?" sorularına cevap aranmıştır. Sonuç olarak, yönetim muhasebecisinin risk yönetim sürecinde aktif olarak görev alması gerektiği kanaatine ulaşılmıştır.

Yerli yazında rastlanan ilk çalışma ise 1999 yılında Karabeyli tarafından yapılmış olan "Risk Denetimi" (Sayıştay) isimli çalışmadır. Çalışmada daha çok kamu denetimi alanına yoğunlaşılmış ve risk odaklı denetim üzerinde durulmuştur.

2004 yılında Özsoy tarafından yapılan ve "Risk Odaklı Denetim ABD Uygulaması ve Türkiye Açısından Değerlendirilmesi" (Active Finans) başlığını taşıyan çalışmada ise bankacılık sektörü açısından risk odaklı denetimin Amerika uygulaması ele alınmış ardından Türkiye uygulaması değerlendirilmiş ve öneriler getirilmiştir.

Mart 2006'da Kishalı ve Pehlivanlı tarafından yapılan "Risk Odaklı İç Denetim ve İMKB Uygulaması" (Muhasebe ve Finansman Dergisi) isimli çalışma ise iç denetime yönelik tanımlayıcı bir araştırma özelliğini taşımakta ve mevcut uygulamaları saptamak için İMKB anket uygulaması içermektedir. Çalışmada risk odaklı denetim sürecinden risk yönetimi temelli denetime geçiş süreci ele alınmıştır.

Bu alanda yapılan en son çalışma ise bir bağımsız denetim kuruluşu olan KPMG Global tarafından The Economic Intelligence Unit'e yaptırılmış ve "Risk ve Kontrollerin Evrimi Hakkında Araştırma Sonuçları" (Uluslararası Kurumsal Yönetim Konferansı) başlığıyla da yayınlanmıştır. Araştırmada son yıllarda risk yönetimi ve iç kontroller alanında meydana gelen gelişmeler ele alınmıştır.

4.2. ÇALIŞMANIN GENEL AMACI

Literatür çalışması kısmında aktarılan bilgiler doğrultusunda ve uluslararası uygulamada iç denetim ve risk yönetim faaliyetlerinin bütünleştirilmesine neden olan

faktörler değerlendirildiğinde, risk yönetimi sistemi alanında meydana gelen gelişmelerden hareketle kurumsal risk yönetimi temelli iç denetim kavramının ortaya çıkmasına neden olan unsurlar bir arada görülebilmektedir.

Uluslararası uygulamanın ulaştığı son durumun dikkate alınması ve Türkiye'de bu konuda neler yapılıyor veya neler yapılmalı sorularının cevapsız kalması bu çalışmanın ortaya çıkmasına zemin hazırlamıştır.

Çizilen bu konu sınırlaması çerçevesinde çalışmanın genel amacı; iç denetim ve kurumsal risk yönetimi faaliyetlerine ilişkin Türkiye uygulamasını gözler önüne sermek, iç denetim faaliyetinin kurumsal risk yönetimi temelli çalışabilmesi için iç denetim ve risk yönetimi sistemlerinin ortak çalışma alanlarını ve veri transferlerinin nasıl gerçekleştirileceğini belirlemektir.

Ayrıca son yıllarda iç denetimin faaliyet alanları arasında ifade edilen risk yönetimi sisteminin denetlenmesi veya kurumsal özelliklere bağlı olarak sistemin işleyişinin iç denetim birimi tarafından organize edilmesi diğer bir ifadeyle yürütülmesi Türkiye penceresinden analiz edilmiştir.

4.3. ÇALIŞMANIN YÖNTEMİ VE KAPSAMI

Çalışmanın genel amaçlarına ulaşabilmek için uygulama kısmı;

- Faaliyet raporları ve kurumsal yönetim uyum raporları incelemesi,
- Anket çalışması,
- Mülakat çalışması

şeklinde üç parça fakat birbirlerini tamamlar şekilde tasarlanmıştır.

Hisse senetleri İMKB'de işlem gören işletmelere ait faaliyet raporları ve kurumsal yönetim uyum raporları; mevcut iç denetim uygulamaları hakkında bir temel oluşturmak, işletmelerin kurumsal yönetim ilkelerini uygulama tavırlarını ve işletme dışı ilgililerin nasıl bilgilendirildiğini belirlemek ve ayrıntılı ele alınan kurumsal risk yönetim sisteminin sınırlarını tespit edebilmek için incelenmiştir.

Rapor incelemesi kazanımları, literatür taraması kısmında sıralanan çalışmaların rehberliğinde ve çalışmanın amacı çerçevesinde genel bir durum tespiti için en uygun yöntem olan anket çalışması, bu çalışmanın uygulama kısmının ikinci

adımı olarak tasarlanmıştır. Hazırlanan anketler İMKB'de hisse senetleri işlem gören işletmelere posta aracılığıyla gönderilmiştir.

Uygulama kısmının son aşaması, mülakat çalışması şeklinde planlanmış ve rapor incelemeleri ve anket çalışması ile elde edilemeyen derinlemesine bilgilere ulaşmak için bir bankanın, reel sektör ağırlıklı faaliyet gösteren bir holdingin ve bir bağımsız denetim firmasının yetkilileriyle mülakatlar gerçekleştirilmiştir. Mülakat çalışması ile özellikle iç denetim ve risk yönetimi faaliyetlerinin etkileşim noktaları, ortak çalışma alanları ve uygulamada denetim evreninin nasıl oluşturulduğu tespit edilmeye çalışılmıştır.

4.4. RAPOR İNCELEMELERİ

Faaliyet raporları ve kurumsal uyumluluk raporları, anket sonuçlarının daha sağlıklı yorumlanabilmesi ve kurumsal yönetim ilkeleri çerçevesinde kamuya açıklanması gereken bir takım bilgilerin, özellikle iç denetim ve risk yönetimi alanında, açıklanıp açıklanmadığının değerlendirilmesi için incelenmiştir.

SPK tebliğleri çerçevesinde hisse senetleri İMKB'de işlem gören şirketler ve BDDK yönetmelikleri çerçevesinde de bankaların faaliyet raporlarını ve kurumsal yönetim uyumluluk raporlarını yayınlamaları gerekmektedir[419].

4.4.1. Rapor İncelemesi Kapsam ve Sınırları

İMKB Ulusal Pazar'da işlem gören şirketler, Yatırım Ortaklıkları, İkinci Ulusal Pazar'da işlem gören şirketler ve yeni ekonomi şirketleri olmak üzere toplamda 320 şirket (Eylül 2007 itibariyle) faaliyet raporları ve kurumsal uyumluluk raporlarının değerlendirilmesi çerçevesinde ana kütle olarak belirlenmiştir. Sözü edilen şirketlere ait faaliyet raporları ve kurumsal uyumluluk raporlarına internet

[419] Borsada işlem gören şirketler, yıllık faaliyet raporları kamuya açıklandıktan sonra (konsolide olmayan mali tablolar ve ekleri kamuya hesap dönemini bitimini izleyen on hafta içinde, konsolide mali tablolar ise on dört hafta içinde kamuya açıklanır) internet sitelerinde yayınlanmak zorundadır ve beş yıl süreyle saklanmalıdır. Bakınız Sermaye Piyasası Kurulu, **"Sermaye Piyasasında Muhasebe Standartları Hakkında Tebliğ",** Seri: XI No: 25, 15.11.2003 tarih ve 25290 sayılı Resmi Gazete, Madde 707 ve 711. Bankalar ise yıllık faaliyet raporunu en geç ilgili hesap dönemi sonunu izleyen yılın Mayıs ayı sonuna kadar matbu olarak ve ayrıca kendi internet sayfalarında finansal tablo kullanıcıları tarafından kolaylıkla ulaşılabilecek şekilde elektronik ortamda yayımlamakla yükümlüdürler. Bakınız BDDK, **"Bankalarca Yıllık Faaliyet Raporunun Hazırlanmasına ve Yayınlamasına İlişkin Usul ve Esaslar Hakkında Yönetmelik",** 1.10.2006 tarih ve 26333 sayılı Resmi Gazete, Madde 10.

sayfaları üzerinden, e-posta yardımıyla veya telefon aracılığıyla ulaşılmaya çalışılmıştır.

Bu raporların yayınlanma zorunlulukları bulunmasına rağmen 88 adet şirkete ait rapora ulaşmak mümkün olmamıştır. Ulaşılamayan raporlar için telefon ve e-posta yöntemiyle işletmelerle iletişim kurulmuş fakat raporlar elde edilememiştir. Ulaşılan rapor sayısı 232 oran olarak ise % 72,5'tir. Bu süreçte işletmelerden gelen cevaplardan bazı işletme üst yönetimlerinin "raporları işletme dışına çıkarmayın" yönünde kararları olduğu öğrenilmiştir. Özellikle İMKB'de grup ve bağlı şirketleri olan bir işletme ile son iki yıl içinde yabancı bir işletme ile birleşme yapmış bir şirketin sözkonusu tutumları ile karşılaşılmıştır.

4.4.2. Rapor İncelemesi Kriterleri

Faaliyet raporları ve kurumsal uyumluluk raporlarının risk yönetimi ve denetim açısından hazırlanıp yayınlama amacına hizmet edebilmesi için yer alması gereken temel bilgiler 11 kategoride toplanabilir. Bunlar aşağıdaki gibi sıralanabilir[420]:

- İç denetim hakkında bilgilerin kolay bulunabilirliği,
- İç kontrol sistemi hakkında bilgi,
- Fonksiyonel - idari raporlama ve bağımsızlık ilişkisi,
- Kurum organizasyon ve yetkilendirmesine ilişkin bilgi,
- Risk odaklı denetim hakkında bilgi,
- Denetim komitesinin bulunup bulunmadığı hakkında bilgi,
- Denetim komitesinin sorumluluk alanları hakkında bilgi,
- İç kontrol, iç denetim ve risk yönetimi sistemine ilişkin denetim komitesinin değerlendirmesinin bulunup bulunmadığı hakkında bilgi,
- Bağımsız denetçinin seçimi sürecine denetim komitesinin dahil edilip edilmediği hakkında bilgi,
- Faaliyet raporuna ilişkin bağımsız denetçinin olurunun bulunup bulunmadığı,

[420] Barma Hanif, **"A Good Story Not Told",** Internal Auditing & Business Risk, October 2005, ss. 20-24.

- İç denetim ve risk yönetimi sürecinde kullanılan bilgisayar yazılımı ve iç denetim birimi raporlarına ilişkin spesifik bilgilerin varlığı.

Rapor incelemelerinde elde edilen veriler Microsoft Excel çalışma sayfalarında karşılaştırılabilir formatta toplanmıştır. Kabul edileceği üzere ilgili raporlara ilişkin inceleme, bu çalışmanın temel uygulaması olan İMKB'de faaliyet gösteren şirketlere ilişkin anket sonuçlarının sağlıklı değerlendirilebilmesi amacıyla bir dayanak noktası oluşturması açısından yapılmıştır. Bu çerçevede elde edilen veriler toplam içindeki ağırlıklarına göre değerlendirilmiştir.

4.4.3. Rapor İncelemesinin Bulguları ve Değerlendirilmesi

Erişilebilen faaliyet ve kurumsal yönetim uyum raporları, 232 adettir. Raporlar, izleyen tabloda yer alan sorular açısından incelenmiş ve sonuçlar tabloda özetlenmiştir. Tabloda, raporlarda cevabı bulunan sorular "evet" aksi halde ise "hayır" olarak kodlanmıştır.

Tablo 16: Rapor İncelemeleri

Araştırma Alanı	Evet (Adet)	Evet (%)	Hayır (Adet)	Hayır (%)
İç Denetim Hakkında Bilgiler Kolaylıkla Bulunabiliyor mu?	111	48	121	52
İç Kontrol Sistemi Var mı?	133	57	99	43
İç Denetim Birimi Fonksiyonel ve İdari Olarak İki Farklı Raporlama Yapıyor mu?	46	19	186	81
Risk Temelli Denetim Uygulanıyor mu?	56	24	176	76
Denetim Komitesi Var mı?	213	92	19	8
Denetim Komitesinin Sorumluluk Alanları Belirlenmiş mi?	72	31	160	69
Denetim Komitesi ile İç Denetim Toplantı Sıklığı Belirtilmiş mi?	54	23	178	87
İç Kontrol, İç Denetim ve Risk Yönetimine İlişkin Denetim Komitesi Değerlendirilmesi Var mı?	16	07	216	93
Denetim Komitesi Bağımsız Denetçinin Seçimi Sürecinde Var mı?	12	05	220	95
Faaliyet Raporuna İlişkin Bağımsız Denetçinin Oluru Var mı?	16	07	216	93

İç denetimde odak nokta başlangıçta kontroller üzerindeyken zamanla denetim temelli riskler ve son olarak da işletme temelli riskler odak nokta haline gelmiştir. İMKB'de faaliyet gösteren şirketlerden % 43'ünde iç kontrol sisteminin bulunmaması bu çalışmanın temelini oluşturan risk yönetimi temelli iç denetimin

Türkiye için henüz erken olduğu şüphesini akıllara getirmektedir. Fakat diğer taraftan BASEL II uzlaşısının yakın bir gelecekte uygulamaya başlanacak olmasının planlanması, COSO Kurumsal Risk Yönetimi Çerçevesinin alanında öncü bazı holdingler tarafından dikkate alınması ve uygulamada rehber olarak kabul görmesi Türkiye uygulamasının uluslararası uygulamanın çok uzağında olmadığına, sınırlı bir kesim tarafından da olsa, işaret etmektedir.

Faaliyet raporları iç denetim biriminin kimlere karşı sorumlu oldukları ve kimlere raporlama yaptıkları açısından incelendiğinde; 46 şirketin (% 19) uluslararası standartta yer alan "iç denetim birimi fonksiyonel olarak denetim komitesine veya yönetim kuruluna idari olarak da yönetim kurulu başkanına raporlama yapar" açıklaması ile uyumlu, diğer 186 şirketin (% 81) ise standart ile çelişen bir tutum takındıkları veya faaliyet raporlarında raporlamaya yönelik herhangi bir açıklamada bulunmadıkları belirlenmiştir.

"Risk Temelli Denetimin Varlığı"nın belirlenebilmesi için faaliyet raporları incelendiğinde ulaşılan sonuç; 56 şirketin (% 24) denetim faaliyetlerine riskleri dahil ettiği yönünde olmuştur. Fakat sözkonusu risklerin denetim temelli riskler mi? olduğu yoksa geniş anlamda şirketlerin karşılaştıkları riskler mi? olduğuna faaliyet raporları incelemesi ile ulaşılamadığından dolayı sorunun cevabı anket çalışmasına bırakılmıştır.

Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ[421] çerçevesinde 213 şirkette (% 92) denetim komitesinin bulunduğu belirlenmiştir. Fakat denetim komitelerinin sorumluluk alanlarının sadece 72 şirket (% 31), iç denetimle yapılan toplantıların sıklıklarının 54 şirket (% 23) tarafından açıklanması ve son olarak da denetim komitesi raporlarına faaliyet raporları arasında yer verilmemesi (sadece 3 şirket yer vermiştir), bu komitelerin yasal düzenlemeye uyum şartı çerçevesinde kurulduğu fakat etkin çalışmadığı gerçeğini gözler önüne sermektedir. Bir diğer önemli nokta da tebliğ ile birlikte denetimden sorumlu komiteler hakkında işletmelerin kamuya açıklama yapmalarının zorunlu hale getirilmemesidir. Bu komitelerin yükümlülüklerini yerine getirip getirmediğine dair

[421] SPK, **Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ,** Seri: X, No: 22, 12.06.2006 tarih ve 29196 sayılı Resmi Gazete, Madde 25.

kamuoyunun bilgilendirilmesi ve bunun da faaliyet raporları ile kurumsal yönetim uyum raporlarında yer alması zorunlu olmalıdır.

Denetim komitelerinin etkin işleyebilmesi üst yönetimin desteği, sorumluluk alanlarının net olarak belirlenmesi ve denetim komitesi üyelerinin komite faaliyetlerine yeterli zamanı ayırmaları halinde mümkün olacaktır. Bu çerçevede incelenen raporların % 31'inde denetim komitesinin sorumluluk alanları ve % 23'ünde ise denetim komitesi ve iç denetim toplantı sıklıkları hakkında bilgi yer almaktadır. Özellikle, Amerika ve Avrupa'da denetim komitesi yönetmeliklerinin ve raporlarının kamuoyu ile paylaşıldığı dikkate alınacak olursa Türkiye uygulaması açısından da en kısa zamanda bu yönde yasal değişikliklerin bir an önce yapılması gereklidir.

Uluslararası uygulamada sıklıkla görülen denetim komitesinin iç kontrol, iç denetim ve risk yönetimine ilişkin değerlendirmelerine yalnızca 16 şirketin (% 7) faaliyet raporlarında yer verildiği ve bunların da tamamının bankalar olduğu belirlenmiştir. Bankaların ilgili yönetmelik çerçevesinde faaliyet raporlarında sözü edilen değerlendirmeyi yapmaları zorunludur. Diğer şirketler için de bu değerlendirmelerin yapılması ve kamuoyuyla paylaşılması zorunluluğu getirilmelidir. Aksi halde ilgili raporların güvenilirlikleri hakkında şüpheler belirebilir. SPK yayınlayacağı tebliğlerle ilk aşamada bu durumu en azından BDDK tebliğleri seviyesine ulaştırmalıdır.

Bir diğer önemli konu da, Enron skandalı sonrası süreçte üzerinde sıklıkla üzerinde durulan ve "denetim komitesi bağımsız denetçiyi seçmeli ve ücretini belirlemeli" görüşünün Türkiye özelinde pek kabul görmediği gerçeğidir. İncelenen faaliyet raporlarından, sadece 12 şirketin (% 5) bağımsız denetçinin seçimi sürecine denetim komitesini dahil ettiği, fakat bunun da tam anlamıyla bağımsız denetçinin seçimi değil, süreçte bulunması anlamında kullanıldığı anlaşılmaktadır.

Son olarak bankalar için BDDK tarafından yayınlanan tebliğe uygun olarak faaliyet raporlarına ilişkin bağımsız denetçinin olurunun alınması uygulanmasına uyulduğu (16 banka-% 7) belirlenmiştir. Temel bir kabul olarak, faaliyet raporlarına ilişkin denetçi olurunun bankacılık sektörü haricindeki şirketler için de zorunlu olması gerekliliği açıktır.

Bu çerçevede Yeni TTK tasarısı'nın 398. madde'sinde şirket veya şirketler topluluğuna ait faaliyet raporlarının bağımsız denetime tabi olması şartı getirilmektedir. Sözkonusu tasarının ilgili maddesinin değişiklik olmaksızın kabulü halinde kurumsal yönetim ilkelerinden en önemlisi olan şeffaflık ilkesi gereğince hareket edilmiş olacak ve şirket hakkında bilgiler kamuoyuna yeterli bir şekilde duyurulmuş olacaktır.

Tasarının yasalaşmasını izleyen süreçte çıkarılacak yönetmeliklerle, şirketlerin hazırlayacakları yıllık raporların asgari içerikleri, kamuoyuna açıklanma tarihleri ve yayınlanma yöntemleri gibi hususlar düzenlenmelidir.

Yukarıda yer alan tespitlere ek olarak incelenen raporlarda iki şirketin iç denetim alanında SAP (Systems Applications and Products in Data Processing) programını ayrıca bir şirketin de COSO KRY çerçevesi temelli çalışan bir bilgisayar programını kullandığı belirlenmiştir. Bir diğer önemli noktada üç şirketin denetim komitesi raporuna faaliyet raporunda yer verdiği ve bir şirketin de yurtdışı yatırım ilişkileri nedeniyle Amerika yasalarına uyum çerçevesinde Sarbanes-Oxley komitesi kurduğu belirlenmiştir. Ayrıca iki şirketin iç denetim raporu başlığı atında, TTK çerçevesinde istihdamı zorunlu olan denetçi raporuna yer verdikleri görülmektedir. Fakat bu raporlar, iç denetim standartlarına paralel hazırlanmamıştır.

4.5. ANKET ÇALIŞMASI

4.5.1. Anket Çalışmasının Kapsamı ve Sınırları

Anket çalışmasının kapsamı, İMKB Ulusal Pazar'da işlem gören şirketler, Yatırım Ortaklıkları, İkinci Ulusal Pazar'da işlem gören şirketler ve yeni ekonomi şirketleri olarak belirlenmiştir. Sözkonusu kapsama dahil 320 şirket ana kütle olarak belirlenmiş ve bütün şirketlere anketler posta aracılığıyla 2007 Haziran ayında gönderilmiştir.

Anketler, faaliyet raporu, kurumsal yönetim uyum raporları ve kurumsal internet sitelerinden belirlenen isimler çerçevesinde ağırlıklı olarak iç denetim birim yöneticilerine, teftiş kurulu başkanlarına veya mali işler koordinatörü pozisyonlarında bulunan yetkililere gönderilmiştir.

4.5.2. Anket Sorularının Hazırlanması ve Soruların Nitelikleri

Anket sorularının hazırlanması sürecinde "Risk and Management Accounting" (Collier, Berry ve Burke), "Enterprise Risk Management: Puling it all together" (Walker, Shenkir ve Barton), "Internal Auditing an Risk Assessment in Large Italian Companies: an Empirical Survey" (Allegrini ve D'onza), "Risk Based Auditing" (Griffiths) ve "Risk Odaklı İç Denetim ve İMKB Uygulaması" (Kishalı ve Pehlivanlı) isimli çalışmaların anket uygulaması ve mülakat çalışması kısımlarından yararlanılmıştır.

Anket soruları hazırlandıktan sonra soruların testi için konunun uzmanı 10 kişilik odak grup oluşturulmuş ve soruların anlaşılabilirliği, homojenliği ve sıralaması test edilmiştir. Odak grup çalışması sonunda sorulara son şekli (Ek I'de yer aldığı şekliyle) verilmiştir.

Anket, kişisel bilgiler (4 soru) ve kurum hakkında bilgiler (23 soru) olmak üzere iki kısımdan ve toplam 27 sorudan oluşmaktadır[422]. Ankette yer alan 16 soru çoktan seçmeli sorulardan ve 11 soru da beşli likert ölçeğine uygun yargı cümlelerinden oluşmaktadır.

4.5.3. Verilerin Toplanması

Haziran 2007'de gönderilen anketler için Ekim 2007'de e-posta aracılığıyla ankete cevap vermeleri yönünde ikinci bir çağrı yapılmıştır. İkinci çağrı öncesinde yaklaşık 60 civarı anket dönmüştür. İkinci çağrı sonrasında adet olarak toplam 79, oran olarak ise % 24,68 (79/320) şirket anketi cevaplandırmıştır. Yakalanan bu oran, uluslararası ortalamanın üzerinde olup, ortalama genelde % 10-13 arasıdır, aynı zamanda denetim alanında yapılan çalışmalarda ulaşılan cevaplanma oranları ile de paralellik göstermektedir[423].

Rapor incelemesi aşamasında ulaşılan bilgilere göre, İMKB'de faaliyet gösteren işletmelerden 56'sı (% 24'ü) Risk Temelli Denetimi uyguladıklarını belirtmişlerdir. Bu sonuçlar aslında çalışmanın konusu itibariyle ana kütle olarak

[422] Lütfen bakınız Ek 1.
[423] Beasley Mark S., Clune Richard and Hermanson Dana R., "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation", **Journal of accounting Public Policy,** Vol: 24, 2005, s. 526.

tanımlanabilecek bir kitlenin ankete cevap verdiğini göstermektedir. Bu durum anket bulgularının değerlendirilmesi kısmında daha da belirgin hale gelmektedir.

Anketlerin geri dönüş sürecinde kimi şirket yetkilileri (3 şirket) telefon veya e-posta aracılığıyla geri dönüş yaparak bu tür anketlere cevap vermediklerini bazı şirketler (5 şirket) ise iç denetim birimleri ve/veya risk yönetimine ilişkin herhangi bir hazırlıkları olmadıkları gerekçesiyle anketleri yanıtlayamayacaklarını bildirmişlerdir.

Cevaplanan anketlerden 3 tanesi uygun verileri içermediği için değerlendirilme dışı bırakılmıştır. Değerlendirilmede dikkate alınan anket sayısı 76'dır. Anketlerin değerlendirilmesi SPSS programı 14.0 versiyonu yardımıyla yapılmıştır.

4.5.4. Güvenilirlik Analizi

Anket cevaplarının ayrıntılı analizine geçmeden önce güvenilirlik yönünden anket sorularının değerlendirilmesi gerekmektedir. Güvenilirlik, ankette yer alan soruların birbirleriyle olan tutarlılığının ve ele alınan sorunu ölçmede homojenliğinin rakam olarak ifade edilmesidir. Güvenilirlik istatistikte çoğunlukla "Cronbach Alfa Katsayısı" ile ölçülmektedir. Katsayı aşağıdaki şekilde sınıflandırılabilir[424]:

$0{,}00 \leq \alpha \leq 0{,}40$ ise ölçek güvenilir değil,
$0{,}40 \leq \alpha \leq 0{,}60$ ise ölçek düşük güvenilirlikte,
$0{,}60 \leq \alpha \leq 0{,}80$ ise ölçek oldukça güvenilir,
$0{,}80 \leq \alpha \leq 1{,}00$ ise ölçek yüksek güvenilirliktedir.

Tablo 17: Güvenirlik İstatistiği

Cronbach's Alpha	N of Items
0,753	21

Tabloda da gözüktüğü gibi anket cevaplarının SPSS programı yardımıyla yapılan ölçümde Cronbach Alfa Katsayısı 0,753 olarak belirlenmiştir. Bu da anketin "oldukça güvenilir" olduğunu göstermektedir.

[424] Akgül Aziz ve Çevik Osman, **İstatistiksel Analiz Teknikleri,** Emek Ofset, Ankara, 2003, s. 435.

4.5.6. Anket Bulgularının Değerlendirilmesi

Ankete ilişkin hipotezlerin testinden önce kurum hakkında bilgilerden hareketle işletmelerin genel görünümleri, iç denetim sistemi ve kurumsal risk yönetimi hakkındaki bilgilere ulaşılmaya çalışılmıştır. Bu kapsamda ankette, kişisel ve kurum hakkında bilgiler kısmında yer alan sorulara verilen cevaplar burada ele alınacaktır.

4.5.6.1. Kişisel Bilgiler ve Görüşler

Anket sıralamasına uygun olarak öncelikle cevaplayıcılar hakkındaki kişisel bilgiler ve görüşler ele alınmıştır.

1. Cevaplayıcılara ünvanları ve deneyimleri sorulmuş ve izleyen tabloda özetlenen sonuçlara ulaşılmıştır.

Tablo 18: Cevaplayıcı Pozisyon Dağılımı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Teftiş Kurulu Başkanı	9	11,8	11,8	11,8
	İç Denetim Müdürü/Elemanı	23	30,2	30,2	42,0
	Genel Müdür	9	11,8	11,8	53,8
	Mali İşler Müdürü	35	46,2	46,2	100,0
	Toplam	76	100,0	100,0	

Anket cevaplayıcıların % 46,2'si mali işler müdürü, % 30,2'si iç denetim müdürü/elemanı % 11,8'er ile de teftiş kurulu başkanı ve genel müdür olarak belirlenmiştir. Bu dağılım iç denetim biriminin aynı zamanda organizasyondaki yerini de göstermektedir.

2. Cevaplayıcılara şu anki pozisyonlarında kaç yıl çalıştıkları sorulmuş ve izleyen tabloda özetlenen sonuçlara ulaşılmıştır.

Tablo 19: Cevaplayıcı Deneyim Dağılımı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	<2	19	25,0	25,0	25,0
	2-5	26	34,2	34,2	59,2
	6-10	18	23,7	23,7	82,9
	11-15	9	11,8	11,8	94,7
	15>	4	5,3	5,3	100,0
	Toplam	76	100,0	100,0	

Cevaplayıcıların deneyim bakımından, ağırlıklı olarak % 34,2 ile 2-5 yıl arası ve % 25 ile de 2 yıldan az deneyime sahip oldukları belirlenmiştir.

3. Cevaplayıcıların riskler karşısındaki eğilimleri belirlenmek istenmiş ve cevap seçenekleri riskleri reddeden, risk almayan, tarafsız, risk alan ve riske karşı istekli şeklinde sınıflandırılmıştır.

Tablo 20: Riskler Karşısındaki Kişisel Eğilim

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Riskleri reddeden	1	1,3	1,4	1,4
	Risk almayan	13	17,1	17,8	19,2
	Tarafsız	24	31,6	32,9	52,1
	Risk alan	35	46,1	47,9	100,0
	Total	73	96,1	100,0	
Kayıp Veri		3	3,9		
Toplam		76	100,0		

Cevaplayıcıların riskler karşısındaki kişisel eğilimlerini belirlemek için sorulan soruya verilen cevaplar değerlendirildiğinde ağırlıklı olarak cevaplayıcıların % 47,9 ile risk alan yapıda oldukları daha sonra ise % 32,9 ile tarafsız oldukları ölçülmüştür.

4. Cevaplayıcılara risk yönetim faaliyetlerinin denetim çalışmalarında ne kadar yer tuttuğu sorulmuş ve izleyen tabloda yer alan sonuçlara ulaşılmıştır.

Tablo 21: İç Denetimde Risk Yönetimi Faaliyetlerine Ayrılan Zaman

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Hiç	1	1,3	1,3	1,3
	% 0-25	23	30,3	30,7	32,0
	% 26-50	23	30,3	30,7	62,7
	% 51-75	18	23,7	24,0	86,7
	% 76-100	10	13,2	13,3	100,0
	Total	75	98,7	100,0	
Kayıp Veri		1	1,3		
Toplam		76	100,0		

İç denetimde risk yönetimi faaliyetlerine ayrılan zamanın belirlenmesi için yöneltilen soruya verilen cevaplar % 30,7'şer ile % 0-25 ile % 26-50 arası şeklindedir.

Bu sonuçlar, iç denetim biriminin KRY sürecindeki etkinliğinin analiz edildiği Tablo 40 ile birlikte değerlendirildiğinde, daha da anlamlı hale gelmektedir.

Sözkonusu tabloda iç denetim biriminin % 50 ile en fazla KRY süreçlerinden raporlama ve izleme aşamasında rol aldığı görülmektedir.

5. İç denetim faaliyetlerinin yüksek etkinlikte gerçekleştirilebilmesi öncelikle üst yönetimin desteğine bağlıdır. Bu çerçevede cevaplayıcılara "İç denetim birimi hakkında üst yönetimin düşüncesi nedir?" şeklinde bir soru yöneltilmiş ve cevaplayıcılardan, çok olumsuz, olumsuz, ilgisiz, istekli ve çok istekli şeklinde beşli sınıflandırma ölçeği yardımıyla yanıtlamaları istenmiş ve izleyen tabloda gösterilen sonuçlara ulaşılmıştır.

Tablo 22: İç Denetim Hakkında Üst Yönetimin Görüşü

	N	Minimum	Maksimum	Ortalama	Standart Sapma
İç denetim hakkındaki üst yönetimin görüşü	73	3,00	5,00	4,3288	0,50152
Valid N (listwise)	73				

Tabloda da gözüktüğü şekliyle üst yönetimin iç denetime bakışı tüm işletmeler açısından "istekli" sınıflandırmasına dahildir. Bu sonuç, iç denetim birimlerinin verilen görevleri etkin bir şekilde gerçekleştirebilmeleri ve bağımsız hareket edebilmeleri açısından önemlidir. Bu sonuç Türkiye'de, en azından İMKB'de yer alan şirketler aısından, iç denetime gerekli desteğin verildiğini göstermektedir.

4.5.6.2. Kurum Hakkında Bilgiler

Anketin ikinci bölümü kurum hakında bilgileri toplamaya yöneliktir. Cevaplayıcıların kurum hakkında bilgiler kısmına verdikleri yanıtların analizi burada yapılmaktadır.

1. Cevaplayıcılara kurumlarının bir grup (holding) şirketi olup olmadığı sorulmuş ve aşağıdaki cevaplar alınmıştır.

Tablo 23: Cevaplayıcıların Kurumlarının Holding İşletmesi Olup Olmadığı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Evet	66	86,8	86,8	86,8
	Hayır	10	13,2	13,2	100,0
	Toplam	76	100,0	100,0	

Anket cevaplayıcılarının % 86,8'i bir grup/holding işletmesi % 13,2'si bağımsız bir işletmedir.

2. Bir önceki soru ile bağlantılı olarak holdinge dahil olan cevaplayıcıların ana şirkette mi yoksa bağlı şirkette mi çalıştıkları belirlenmek istenmiş ve izleyen tablodaki cevaplara ulaşılmıştır.

Tablo 24: Kurumun Holding İçindeki Yeri

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Ana Şirket	16	21,1	24,2	24,2
	Bağlı Şirket	50	65,8	75,8	100,0
	Total	66	86,8	100,0	
Kayıp Veri		10	13,2		
Toplam		76	100,0		

Bir holdinge bağlı olduklarını belirten cevaplayıcılardan % 24,2'si ana şirkette % 75,8'i ise bağlı şirkette faaliyette bulunmaktadırlar. Bu sonuçlar kurumsal işletmelerin denetime ve risk yönetimi faaliyetlerine imkânlar doğrultusunda yeterli ölçüde kaynak ayırıp bu faaliyetleri önemsediklerini göstermektedir.

3. Cevaplayıcılara hangi sektörde faaliyet gösterdikleri sorusu yöneltilmiş ve izleyen tabloda yer alan sonuçlara ulaşılmıştır.

Tablo 25: Sektörel Dağılım

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Finans/Bankacılık	26	34,2	34,2	34,2
	Üretim/Perakende	42	55,2	55,2	89,6
	Hizmet	7	9,2	9,2	98,8
	Teknoloji	1	1,3	1,3	100,0
	Toplam	76	100,0	100,0	

Ankete katılanların % 34,2'si Finans/Bankacılık, % 55,2'si Üretim/Perakende, % 9,2'si Hizmet, % 1,3'ü Teknoloji sektöründe faaliyette bulunmaktadır.

4. Cevaplayıcılara kurumlarında çalışan sayısı sorulmuş ve izleyen tabloda özetlenen sonuçlara ulaşılmıştır.

Tablo 26: Çalışan Sayısı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	250 ve altı	19	25,0	25,0	25,0
	251-500	13	17,1	17,1	42,1
	501-1000	12	15,8	15,8	57,9
	1001-2500	14	18,4	18,4	76,3
	2501 ve üstü	18	23,7	23,7	100,0
	Toplam	76	100,0	100,0	

Ankete cevap veren işletmeler içinde % 25 ile ağırlıklı olarak çalışan sayısının "250 ve altı" olduğu bunu % 23,7 ile "2501 ve üstü" çalışana sahip işletmelerin izlediği tablodan anlaşılmaktadır.

5. Cevaplayıcılara çalıştıkları kurumların aktif büyüklükleri sorulmuş ve izleyen tabloda gösterilen sonuçlara ulaşılmıştır.

Tablo 27: İşletme Aktif Büyüklükleri

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	3milyon YTL'den-15 m YTL'ye kadar	6	7,9	7,9	7,9
	15 m YTL'den-50 m YTL'ye kadar	8	10,5	10,5	18,4
	50 m YTL'den-200 m YTL'ye kadar	18	23,7	23,7	42,1
	200 m YTL ve üstü	44	57,9	57,9	100,0
	Toplam	76	100,0	100,0	

Ankete cevap veren işletmelerin ağırlıklı olarak % 57,9 ile 200 milyon YTL ve üstü aktif büyüklüğüne sahip işletmelerden oluştuğu tablodan anlaşılmaktadır.

6. Cevaplayıcılara "Kurumunuzda iç denetim birimi var mı?" sorusu yöneltilmiş ve izleyen tabloda aktarılan sonuçlara ulaşılmıştır.

Tablo 28: İç Denetim Biriminin Varlığı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Evet	64	84,2	84,2	84,2
	Hayır	12	15,8	15,8	100,0
	Toplam	76	100,0	100,0	

Bu çalışmanın özünü iç denetim birimine sahip işletmeler oluşturmaktadır. Ankete katılan işletmelerin % 84,2'sinde iç denetim birimi bulunduğu % 15,8'inde ise iç denetim biriminin bulunmadığı anlaşılmaktadır.

7. Cevaplayıcılara kurumlarındaki iç denetçi sayıları sorulmuş ve izleyen tabloda gösterilen sonuçlara ulaşılmıştır.

Tablo 29: İç Denetçi Adedi

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	1-3	34	44,7	44,7	44,7
	4-7	14	18,4	18,4	63,2
	8-12	3	3,9	3,9	67,1
	13-18	3	3,9	3,9	71,1
	18 ve üstü	8	10,5	10,5	81,6
	Yok	14	18,4	18,4	100,0
	Toplam	76	100,0	100,0	

Kurumlarında iç denetçi istihdam eden işletmeler (76-14) 62'dir. İç denetim departmanına sahip işletmelerden (34/62) % 56,3'ünün 1-3 ve % 21,9'unun de 4-7 arası denetim elemanına sahip olduğu tablodan anlaşılmaktadır.

8. Cevaplaycılara "Dış kaynaktan denetim destek hizmeti alıyor musunuz?" sorusu yöneltilmiş ve izleyen tabloda gösterilen sonuçlara ulaşılmıştır.

Tablo 30: Dış Kaynaktan Denetim Hizmet Alımı

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Evet	57	75,0	75,0	75,0
	Hayır	19	25,0	25,0	100,0
	Toplam	76	100,0	100,0	

Anket katılımcılarından % 75'i dış kaynaktan denetim destek hizmetleri aldıklarını belirtmişlerdir.

9. Bir önceki soruyla bağlantılı olarak dış kaynaktan alınan denetim destek hizmetlerinin neler olduğu sorulmuş ve izleyen tabloda aktarılan sonuçlara ulaşılmıştır.

Tablo 31: Dış Kaynaktan Alınan Denetim Destek Hizmetleri

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Bilgi teknolojileri denetimi	9	15,8	15,8	15,8
	Yabancı ülke şubeleri denetimi	3	5,3	5,3	21,1
	Geçici özel görevlendirmeler (hile incelemeleri vb)	2	3,5	3,5	24,6
	İç denetim bütünleştirme çalışmaları	8	14,0	14,0	38,6
	Diğer	35	61,4	61,4	100,0
	Toplam	76	100,0	100,0	

Tablodan da görülebileceği gibi tek alanda alınan denetim destek hizmeti; % 15,8 ile bilgi teknolojileri denetimi ve % 14,0 ile iç denetim bütünleştirme çalışmalarıdır. Dış kaynaktan denetim destek hizmetleri alanların % 61,4'ü diğer seçeneğini tercih etmiştir. Bu çalışmanın amacı işletmelerin dışarıdan aldıkları iç denetim hizmetlerini ve risk yönetimi ayrıntılı incelemektir, fakat diğer seçeneğini tercih edenlerin % 90'ını yeminli mali müşavirlik hizmeti oluşturduğu anket sonuçlarının incelenmesinden anlaşılmaktadır.

KPMG bağımsız denetim firması tarafından küresel ölçekte yapılan araştırmaya göre, katılımcıların % 39'u iç denetimin en az bir bölümünü dış kaynaktan sağladıklarını belirtmişlerdir. Türkiye sonuçlarında ise bu oran % 75 çıkmış, fakat dış kaynaktan alınan denetim destek hizmetlerinin ağırlıklı olarak yeminli mali müşavirlik hizmeti alımı olduğu belirlenmiştir[425].

10. İç denetim biriminin organizasyon içinde hangi ilgiliye raporlama yaptığının tespiti için sorulan soruda cevaplayıcılara birden fazla tercih hakkı verilmiştir seçenekler yönetim kurulu başkanı, yönetim kurulu üyesi, CEO, denetim komitesi, ve genel müdür veya yardımcıları şeklinde sıralanmıştır. Birden fazla tercih hakkı verilmesinin nedeni iç denetim biriminin fonksiyonel ve idari olarak raporlama yaptığı ilgilileri dikkat çekmeden belirleyebilmektir.

[425] Yardımcı Ebru, **"Risk ve Kontrollerin Evrimi Hakkında Araştırma Sonuçları",** Uluslararası Kurumsal Yönetim Konferansı, 15 Ocak 2008, İstanbul, s. 10.

Tablo 32: İç Denetim Biriminin Raporlama Yaptığı Yetkililer

	Sıklık	Rapor Sayısı Ortalaması
a) Yönetim Kurulu Başkanı	30	
b) Yönetim Kurulu Üyesi	16	
c) CEO	16	6.5
d) Denetim Komitesi	23	
e) Genel Müdür veya Yardımcıları	29	

Standartta önerilen, iç denetim biriminin fonksiyonel olarak denetim komitesine veya yönetim kurulunun ilgili üyesine, idari olarak da yönetim kurulu başkanına raporlama yapmasıdır. Fakat ulaşılan sonuçlar uygulamada Genel Müdür veya yardımcıları ile CEO'ya yapılan raporlamaların toplama oranı (45/114) % 39 olarak bulunmuştur. Diğer yandan Denetim Komitesi ve ilgili Yönetim Kurulu Üyesi'ne yapılan raporlamaların toplama oranı (39/114) % 34 olarak belirlenmiştir. Bu durum uluslararası uygulama ve standart ile çelişmektedir.

Yıllık raporlama ortalaması ise 6.5 bulunmuştur. Bu da yılda en az 6 kez iç denetim raporu hazırlandığı anlamına gelmektedir. Uygulama bölümünün ilk adımı olan faaliyet raporu incelemesinde; Türkiye'de iç denetim raporlarının kamuya açıklanmadığı, yayınlanmadığı ve internet yoluyla yatırımcılara ve diğer ilgililere duyurulmadığı sonucuna ulaşılmıştır. İç denetim raporlarının, düzenli aralıklarla yayınlanmasının şeffaflık açısından yararlı olacağı açıktır.

Türkiye uygulamasının aksine 2007 yılında PricewaterhouseCoopers tarafından Amerika'da yapılan araştırmaya göre cevaplayıcıların % 86'sı denetim komitesine veya yönetim kurulu başkanına fonksiyonel anlamda raporlama yaptıklarını belirtmişlerdir. İdari raporlamanın ise % 31 oranında CEO'ya ve % 47 oranında CFO (Chief Financial Officer)'ya yapıldığı belirlenmiştir[426].

Türkiye uygulamasında Denetim Komitesi ve ilgili Yönetim Kurulu Üyesi'ne yapılan fonksiyonel raporlamanın % 34 oranında bulunması, öte yandan Amerika uygulamasında ise bu oranın % 86 olması, Amerika uygulamasının Türkiye uygulamasına kıyasla iç denetim birimlerine daha çok bağımsız hareket etme kabiliyeti verdiğini ve aynı zamanda standartla paralel olduğunu göstermektedir.

[426] PricewaterhouseCoopers, **Internal Audit 2012,** s. 42.

11. Cevaplayıcılara iç denetim faaliyetlerinin odak noktası sorulmuş ve yanıtlarını 1-5 aralığındaki beşli ölçeğe aktarmaları istenmiştir.

Tablo 33: İç Denetim Faaliyetinin Odak Noktası

	N	Ortalama	Standart Sapma
İşletme riskleri temelli denetim	61	3,6393	1,27845
Finansal tabloların denetimi	68	3,8824	1,16580
Faaliyet denetimi	68	4,1471	0,77776
Uygunluk denetimi	65	4,3077	0,68290
Bilgi teknolojileri denetimi	63	2,8889	1,36914
Kurumsal Risk Yönetimi faaliyetleri	72	3,1944	1,28522
Hata araştırmaları	65	3,8000	1,04881
Valid N (listwise)	59		

Yanıtlardan anlaşıldığı üzere iç denetim faaliyetlerinin odak noktası ağırlıklı olarak 4,30 ortalama ile uygunluk denetimindedir. Uygunluk denetimini ise 4,14 ortalama ile faaliyet denetimi, 3,88 ortalama ile finansal tabloların denetimi, 3,80 ortalama ile hata araştırmaları, 3,63 ortalama ile işletme risklerinin denetimi ve son olarak da 2,88 ortalama ile bilgi teknolojilerinin denetimi izlemektedir. Bu sonuçlar Tablo 44 "Kurum Denetim Kültürünün Tanımlanması" ile birlikte değerlendirildiğinde daha anlamlı hale gelmektedir.

12. Cevaplayıcılara "Kurumunuzda Kurumsal Risk Yönetimi (KRY) çalışmaları hangi aşamadadır?" sorusu yöneltilmiş ve izleyen tabloda gösterilen sonuçlara ulaşılmıştır.

Tablo 34: KRY Safhası

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Tam olarak faal	28	36,8	36,8	36,8
	KRY süreci başladı ama tam olarak faal değil	28	36,8	36,8	73,7
	Planlama aşamasında	13	17,1	17,1	90,8
	Henüz düşünülmemekte	7	9,2	9,2	100,0
	Toplam	76	100,0	100,0	

Tablodan da görülebileceği gibi KRY'nin tam olarak faal olduğu (% 36,8) ve KRY sürecinin başladığı ama tam olarak faal olmadığı (% 36,8) işletmeler cevaplayıcıların % 73,6'sını oluşturmaktadır. KRY sürecinin tam olarak faal olduğu kurumların yasal zorunluluk nedeniyle bankalar (ankete katılan banka/finansal kurum adedi 26'dır) ve diğerlerinin de uluslararası arenada rekabeti en üst düzeyde

yaşayan kurumlar olan holdingler ve iştirakleri olduğu anket geri dönüşlerine paralel olarak tekrar incelenen faaliyet raporlarından anlaşılmaktadır.

13. Anket cevaplayıcılarının risk yönetim faaliyetlerine *yön veren etkenler* hakkındaki düşünceleri sorulmuş ve cevap seçenekleri yasal etkenler, ortakların beklentileri, ticaret hayatının rekabet ortamı, müşteri/tüketici talepleri, yönetim kurulu/üst yönetim talepleri, kurumsal yönetim ilkeleri, uluslararası standart veya çerçeveler (IIA, COSO) ve diğer olarak sıralanmıştır. Cevaplar izleyen tabloda özetlenmiştir.

Tablo 35: Risk Yönetim Faaliyetine Yön Veren Etkenler

Kurumunuzda risk yönetim faaliyetlerine *yön veren etkenler* hakkındaki düşünceleriniz:	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
a) Yasal etkenler	% 1,4	% 2,7	% 12,2	% 59,5	% 24,3
b) Ortakların beklentileri	% 2,8	% 4,2	% 5,6	% 66,2	% 21,2
c) Ticaret hayatının rekabet ortamı	% 1,4	% 2,8	% 9,9	% 59,2	% 26,8
d) Müşteri/tüketici talepleri	% 1,4	% 15,9	% 17,4	% 43,5	% 21,7
e) Yönetim kurulu/üst yönetim talepleri	% 1,4	% 2,7	% 12,2	% 59,5	% 24,3
f) Kurumsal yönetim ilkeleri	% 2,7	% 1,4	% 9,5	% 60,8	% 25,7
g) Uluslararası standart veya çerçeveler (IIA, COSO)	% 2,9	% 7,1	% 12,9	% 55,7	% 21,4
h) Diğer					

Katılımcılar genel olarak soru seçeneklerinde verilen tüm faktörlerin risk yönetimi faaliyetlerine yön verdiklerini belirtmişlerdir. Bunun yanısıra ortakların beklentileri % 87,4 ve kurumsal yönetim ilkelerinin % 86,5 ile (Katılıyorum ve Kesinlikle Katılıyorum oranlarının toplamı) diğer faktörlere kıyasla risk yönetimi faaliyetlerine daha fazla yön verdikleri anlaşılmaktadır. Diğer yandan sıralanan faktörlerden müşteri/tüketici taleplerinin % 17,3 ve uluslararası standart veya çerçevelerinin % 9 ile (Kesinlikle Katılmıyorum ve Katılmıyorum oranlarının toplamı) risk yönetim faaliyetlerine en az yön verdiği görüşü anket sonuçlarından anlaşılmaktadır. Tablo değerlendirilirken Katılıyorum ve Kesinlikle Katılıyorum ile Kesinlikle Katılmıyorum ve Katılmıyorum seçeneklerinin toplamları dikkate alınmış ve bunların arka fonu siyah olarak gösterilmiştir.

14. Cevaplayıcılara "Kurumunuzun risk alma tutumunu nasıl tanımlayabilirsiniz?" sorusu yöneltilmiş ve verilen cevaplar izleyen tabloda gösterilmiştir.

Tablo 36: Kurum Risk Alma Tutumu

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Riskleri reddeden	1	1,3	1,3	1,3
	Risk almayan	13	17,1	17,1	18,4
	Tarafsız	15	19,7	19,7	38,2
	Risk alan	44	57,9	57,9	96,1
	Risklere karşı istekli	3	3,9	3,9	100,0
	Toplam	76	100,0	100,0	

Sonuçlardan % 61,8 cevaplayıcının kurum risk alma tutumlarını "risk alan" veya "risklere karşı istekli" şeklinde tanımladıkları anlaşılmaktadır. Öte yandan "riskleri reddeden" veya "risk almayan" seçeneklerinin tercih edenlerin oranları toplamı % 18,4 olarak belirlenmiştir. Bu durum ağırlıklı olarak kurumların risk alan yapıda olduklarını gözler önüne sermektedir.

15. Cevaplayıcılara "Son iki yıl içinde kurumunuzda risk tanımlama çalışmaları yapıldı mı?" sorusu yöneltilmiş ve aşağıdaki cevaplara ulaşılmıştır.

Tablo 37: Risk Tanımlama Çalışmaları

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Evet	48	63,2	63,2	63,2
	Hayır	28	36,8	36,8	100,0
	Toplam	76	100,0	100,0	

Günümüzde küreselleşmenin hız kazanması, krizlerin daha hızlı bir şekilde bütün dünyada hissedilir hale gelmesi ve diğer etkenler risk tanımlamalarının sık aralıklara güncelleştirilmesini zorunlu kılmaktadır. Bu bağlamda katılımcılara yöneltilen soruya verilen cevaplardan son iki yılda risk tanımlama çalışmalarının % 63,2 oranında yapıldığı belirlenmiştir.

16. Risk tanımlama çalışmalarının kim tarafından yapıldığının tespiti için yöneltilen soruya verilen cevaplar izleyen tabloda gösterilmiştir.

Tablo 38: Risk Tanımlama Çalışmalarını Gerçekleştiren İlgililer

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Kurum dışı danışmanlar tarafından	3	6,3	6,3	6,3
	Risk yönetim birimi tarafından	15	31,3	31,3	37,5
	İç denetim birimi tarafından	7	14,6	14,6	52,1
	Yöneticilerin katıldığı beyin fırtınası çalışmaları sonucunda	6	12,5	12,5	64,6
	Diğer	17	35,4	35,4	100,0
	Toplam	48	100,0	100,0	

Cevaplardan risk tanımlama çalışmalarının ağırlıklı olarak, % 31,3 oranında, risk yönetim birimi tarafından yapıldığı iç denetim biriminin ise % 14,6 oranında bu çalışmaları yürüttüğü anlaşılmaktadır. Ayrıca diğer seçeneğini tercih edenlerin % 19'unun risk tanımlamalarını risk yönetim ve iç denetim birimleri tarafından ortaklaşa yürüttüklerini ve yaklaşık % 25'inin de risk tanımlamalarını iç denetim birimi elemanları ve yöneticilerin katıldıkları beyin fırtınası çalıştayı ile belirledikleri anket sonuçlarının ayrıntılı incelenmesiyle anlaşılmıştır.

17. Ankette 2.17 no'lu soru olarak tasarlanan ve genel olarak KRY faaliyetlerinden kimin sorumlu olduğunun tespiti için yöneltilen soruya verilen cevaplar izleyen tabloda yer almaktadır.

Tablo 39: KRY Sorumluluğu

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	CEO/Genel Müdür	23	30,3	39,0	39,0
	Yönetim Kurulu	17	22,4	28,8	67,8
	Finans Direktörü	5	6,6	8,5	76,3
	İç Denetim Müdürü	6	7,9	10,2	86,4
	Risk Yöneticisi	6	7,9	10,2	96,6
	Hat Yönetimi	2	2,6	3,4	100,0
	Total	59	77,6	100,0	
Kayıp Veri		17	22,4		
Toplam		76	76	100,0	

KRY faaliyetlerinden ağırlıklı olarak % 30,3 oranında CEO/Genel Müdürlerin sorumlu olduğu bunları ise % 22,4 ile Yönetim Kurulunun izlediği anlaşılmaktadır. KRY faaliyetlerinde iç denetim müdürlerinin ve risk yöneticilerinin % 7,9 olarak aynı oranda sorumlu oldukları belirlenmiştir. Tablodan da görülebileceği gibi "Kayıp Veri" olarak ifade edilen anket katılımcılarının bu soruya

cevap vermeme sayısı 17'dir. Bu değer Tablo 34 "Kurumsal Risk Yönetimi Safhası" ile birlikte değerlendirildiğinde anlaşılır hale gelmektedir. Tablo 34'te KRY safhası ele alınmış ve toplamda 20 kurumun ya KRY sistemini kullanmadığı ya da henüz planlama aşamasında olduğu sonucuna ulaşılmıştır. Diğer bir ifadeyle KRY sorumluluğunun araştırıldığı soruya cevap vermeyen 17 katılımcının kurumunda ya KRY kullanılmamakta ya da henüz planlama aşamasındadır.

18. Cevaplayıcıların kurumlarında "risk tanımlama", "risklerin analizi ve değerlendirilmesi", "risk tutumunun belirlenmesi", "raporlama ve izleme" ve "genel olarak kurumsal risk yönetimi faaliyetleri"nin yürütülmesi sürecinde iç denetim biriminin etkinliğinin belirlenmesi için tasarlanan soruya verilen cevaplar izleyen tabloda özetlenmektedir.

Tablo 40: İç Denetim Biriminin KRY Sürecindeki Etkinliği

KRY Süreci	İç Denetim Müdürü / Elemanı (Adet)	İç Denetim Müdürü / Elemanı (%)	Diğer İlgili (Adet)	Diğer İlgili (%)
Risk Tanımlama	12	22,6	41	77,4
Risklerin Analizi ve Değerlendirilmesi	15	26,3	42	73,7
Risk Tutumunun Belirlenmesi	8	10,5	45	59,2
Raporlama ve İzleme	33	50,0	33	50,0
Genel Olarak KRY Faaliyetleri	9	15,0	51	85,0

Katılımcı cevaplarının özetlendiği tabloda da görüldüğü gibi iç denetim biriminin yoğun bir biçimde yürüttüğü destek verdiği kurumsal risk yönetimi alanı % 50 ile raporlama ve izlemedir. Raporlama ve izleme faaliyetini % 26,3 ile risklerin analizi ve değerlendirmesi, % 22,6 ile risk tanımlama, % 15 ile genel olarak kurumsal risk yönetimi faaliyetleri ve son olarak da % 10,5 ile risk tutumunun belirlenmesi takip etmektedir.

Raporlama ve izleme faaliyetlerinin ilgili birim dışından bağımsız ve objektif bir şekilde yürütülmesi kurumsal yönetim ilkelerinden şeffaflık ve objektifliğin bir gereğidir. Bu çerçevede ilerleyen yıllarda risk yönetim sistemlerinin raporlama ve izleme faaliyetlerinin daha yüksek oranlarda iç denetim birimlerine bırakılması beklenmektedir.

Yukarıda ifade edilen faaliyetleri yürüten diğer ilgililer ise CEO/Genel Müdür, Yönetim Kurulu/Denetim Komitesi, Finans Direktörü/Elemanı, Risk Yöneticisi/Elemanı, Hat Yönetimi/Elemanı şeklinde sınıflandırılmıştır.

Bu bilgiden hareketle risk tanımlama faaliyetlerini yürüten diğer ilgililerden (41 kişi) % 56'sının Finans Direktörü/Elemanı % 39'unun da Risk Yöneticisi/Elemanı olduğu belirlenmiştir.

Risklerin analizi ve değerlendirilmesi işlemini yürüten diğer ilgililerden (42 kişi) % 61'inin Finans Direktörü/Elemanı, % 30'unun ise Risk Yöneticisi/Elemanı olduğu belirlenmiştir.

Risk tutumunun belirlenmesi iç denetim standartında da geçtiği şekliyle bir üst yönetim faaliyetidir ve sorumluluğu da üst yönetime aittir. İç denetim birimi risk tutumunun belirlenmesi sürecinde danışman rolünün dışına çıkmamalıdır. Standart çerçevesinde uygulamada da risk tutumunun daha çok CEO/Genel Müdür (% 66) ve Yönetim Kurulu/Denetim Komitesi (% 17) tarafından belirlendiği sonucuna ulaşılmıştır.

Raporlama ve izleme faaliyetlerini yürüten diğer ilgililer (33 kişi) ise Finans Direktörü/Elemanı (% 25) ve Risk Yöneticisi/Elemanı (% 25) şeklinde belirlenmiştir.

Genel Olarak Kurumsal Risk Yönetimi faaliyetlerini yürüten diğer ilgililer (51 kişi) CEO/Genel Müdür (% 47) ve Yönetim Kurulu/Denetim Komitesi'nin (% 31) olduğu belirlenmiştir.

Daha önce de ifade edilen PricewaterhouseCoopers tarafından küresel ölçekte yapılan araştırmada; kurumsal risk yönetimi faaliyetlerinin sorumluluğunun organizasyon düzeyinde kimde olduğu araştırılmış ve % 32 oranında cevaplayıcının sorumluluk iç denetim birimindedir cevabını verdikleri belirlenmiştir[427]. Bu araştırma çerçevesinde, Türkiye araştırması, ise iç denetim birimlerinin kurumsal risk yönetimi faaliyetlerinin sorumluluğunu % 15 oranında üstlendikleri görülmektedir. PricewaterhouseCoopers araştırmasına göre risk değerleme faaliyetlerinin % 36 oranında iç denetim birimi tarafından yapıldığı dikkatleri çekmektedir[428]. Türkiye'de ise risk değerlemelerinin % 26 oranında iç deneçiler tarafından yapıldığı sonucuna ulaşılmıştır. Türkiye'de iç denetim aleyhine olan bu farkın ilerleyen yıllarda kapanacağı tahmin edilmektedir.

[427] PricewaterhouseCoopers, **Internal Audit 2012,** s. 9.
[428] **a.g.e.,** s. 9.

19. Anketin 2.19 no'lu sorusu olarak tasarlanan ve cevaplayıcılara "İç denetim planı hazırlanırken dikkate alınan riskler nelerdir?" şeklinde yöneltilen soruya verilen cevaplar aşağıdaki gibidir.

Tablo 41: İç Denetim Planı Hazırlanırken Dikkate Alınan Riskler

	Evet	Hayır	Dikkate Alınma Yüzdesi
Finansal Riskler	68	8	89,4
Operasyonel Riskler	64	12	84,2
Stratejik Riskler	41	35	53,9
İtibar Riski	36	40	47,3
Bilgi Teknolojileri Riski	36	40	47,3
Düzenleme Riski	26	50	34,2

İç denetim planı hazırlanırken dikkate alınan risklere yönelik soruya cevaplayıcıların; % 89,4'ü finansal riskleri, % 84,2'si operasyonel riskleri, % 53,9'u stratejik riskleri, % 47,3'ü itibar risklerini yine % 47,3'ü bilgi teknolojileri risklerini ve son olarak % 34,2'si de düzenleme riskini dikkate aldıklarını belirtmişlerdir.

Bu soru KRY'nin iç denetim üzerindeki etkisinin belirlenmesi için sorulmuş ve beklendiği şekliyle iç denetim biriminin spesifik risklerde dahil olmak üzere pek çok riskle ilgilendiği ve denetimin planlanması aşamasında dikkate alındığı sonucuna ulaşılmıştır. Ulaşılan sonuçlar KRY ve iç denetimin bütünleştirilmesi sürecinde olumlu gelişmelerin yaşandığını göstermektedir.

20. Cevaplayıcıların risk yönetiminde ne tür araçlar kullandıkları belirlenmek istenmiştir. Bu çerçevede cevaplayıcılara[429]; literatürde temel risk yönetimi araçları olarak bilinen;

- Beyin fırtınası, senaryo analizleri ve SWOT analizleri,
- Görüşme ve anket,
- Olasılık/etki matrisi ile

risk yönetiminde sıklıkla başvurulan teknik araçlar olarak bilinen;

- Stokastik modelleme ve istatistiksel analizler,
- Risk yönetim yazılımı

[429] Collier, Berry and Burke, **Risk and Management Accounting,** s. 59.

alternatifleri verilmiştir. Yukarıda yapılan sınıflandırma ve ankette yer alan bu soru Collier, Berry ve Burke tarafından "Risk and Management Accounting" isimli çalışmadan esinlenilerek hazırlanmıştır.

Bu sorunun cevaplanması için cevaplayıcılara 1-5 arası beşli likert ölçeği verilmiş ve alınan cevaplar izleyen tabloda bir arada gösterilmiştir.

Tablo 42: Kullanılan Risk Yönetimi Teknikleri

	N	Minimum	Maksimum	Ortalama	Standart Sapma
Deneyim, Yargı	63	2,00	5,00	4,0000	0,84242
İç Denetçi veya Bağımsız Danışman Kullanımı	59	1,00	5,00	3,8475	1,11128
Beyin Fırtınası, Senaryo Analizleri, SWOT Analizleri	***62***	***1,00***	***5,00***	***3,7581***	***1,00304***
Görüşme, Anket	***57***	***1,00***	***5,00***	***3,1228***	***1,26872***
Olasılık/Etki Matrisi	***58***	***1,00***	***5,00***	***3,0690***	***1,29591***
Stokastik Modelleme ve İstatistiksel Analizler	55	1,00	5,00	3,2364	1,23174
Risk Yönetim Yazılımı	46	1,00	5,00	2,6739	1,59240

Risk yönetimi tekniklerinin temel ve teknik ayrımının yanısıra cevap seçenekleri arasında yer alan "Deneyim, Yargı" ve "İç denetçi veya bağımsız danışman kullanımı" ayrı başlıklar halinde ele alındığında aşağıdaki sonuçlara ulaşılmaktadır.

	Ortalama
Temel Yöntemler	3,32
Teknik Yöntemler	2,95
Deneyim, Yargı	4,00
İç Denetçi veya Bağımsız Danışman Kullanımı	3,85

Bu sonuçlardan hareketle Deneyim ve Yargı 4,00 ortalama ile en çok başvurulan yöntem iken, bunu 3,85 ortalama ile İç Denetçi veya Bağımsız Danışman kullanımı izlemektedir. Temel Yöntemlerin kullanılma oranı 3,32 olarak belirlenirken Teknik Yöntemler ise 2,95 ortalama ile sonuncu yöntem olmuştur.

Bu sonuçlar Türkiye'de risk yönetimi sürecinde ağırlıklı olarak deneyim ve yargılara göre hareket edildiği veya iç denetçi-bağımsız danışman kullanımına

gidildiğini göstermektedir. Diğer bir ifadeyle risklerin ölçümünde sayısal tekniklerden ziyade tecrübeler ve kişisel yargılar daha çok ön plandadır.

21. Cevaplayıcılara "*İşletme Temelli Riskler* kurumunuz iç denetim faaliyetlerinde hangi aşamalarda dikkate alınmaktadır?" sorusu yöneltilmiş ve verilen cevaplar izleyen tabloya aktarılmıştır.

Tablo 43: İşletme Temelli Risklerin Denetimde Kullanıldığı Aşamalar

		Sıklık	Yüzde	Geçerli Yüzde	Kümülatif Toplam
Geçerli	Dikkate alınmamakta	10	13,2	13,2	13,2
	Planlama aşamasında	16	21,1	21,1	34,2
	Raporlama ve izleme aşamasında	11	14,5	14,5	48,7
	Bütün aşamalarda	39	51,3	51,3	100,0
	Toplam	76	100,0	100,0	

Yukarıdaki tablodan da anlaşıldığı gibi % 51,3 oranında anket katılımcısı iç denetimin bütün aşamalarında işletme temelli risklerin dikkate alındığını belirtmişlerdir. % 13,2 oranında katılımcı ise işletme temelli risklerin iç denetim faaliyetlerinde dikkate alınmadığını belirtmişlerdir.

22. Anketin son sorusu olarak tasarlanan ve Walker, Shenkir ve Barton tarafından yapılan "Enterprise Risk Management: Pulling it all Together" isimli çalışmadan esinlenilen "Kurumunuz denetim kültürünü 4 farklı açıdan nasıl tanımlayabilirsiniz?[430]" sorusunu cevaplayıcıların "Denetim Yaklaşımı", "Denetçinin Rolü", "Denetimin Odak Noktası" ve "Denetçi Nitelikleri" açılarından yanıtlamaları istenmiştir. Bu sorunun cevaplanması için cevaplayıcılara 1-5 arası beşli likert ölçeği verilmiş ve alınan cevaplar izleyen tabloda bir arada gösterilmiştir.

Tablo 44: Kurum Denetim Kültürünün Tanımlanması

	N	Minimum	Maksimum	Ortalama	Standart Sapma
Denetim Yaklaşımı	73	1,00	5,00	3,6986	1,13877
Denetçinin Rolü	73	1,00	5,00	3,8630	,88687
Denetimin Odak Noktası	73	1,00	5,00	3,6438	1,04576
Denetçi Nitelikleri	73	1,00	5,00	3,4795	1,10692
Geçerli N (listwise)	73				

Cevaplayıcı düzeyinde toplam skor;

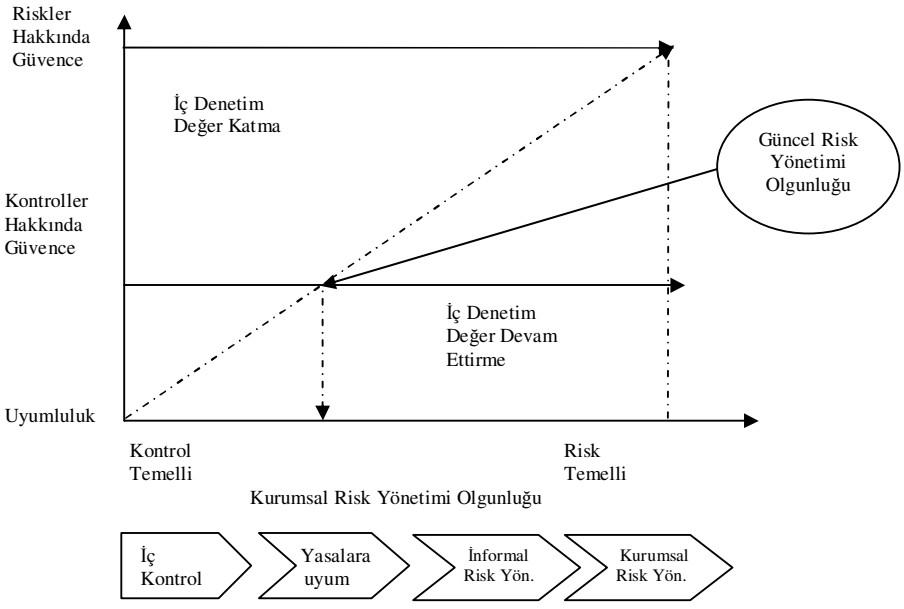
[430] Walker Paul L., Shenkir William G. and Barton Thomas L., **Enterprise Risk Management: Pulling it all Together,** s. 147.

- 15-20 arası ise işletme iç denetim departmanının KRY çalışmalarını yürüttüğü veya danışman öncü rolü üstlendiği veya KRY temeli iç denetime hazır olduğunu,
- 10-14 arası ise henüz iç denetim biriminin KRY temelli çalışmadığı fakat bu yönde bir çabasının bulunduğunu
- 4-9 arası ise risk yönetimi sisteminin sigorta temelli çalışan bir fonksiyon olarak ele alındığını göstermektedir.

Dört farklı açıdan yapılan değerlemelerin ortalamalarının toplamı 14,68 olarak bulunmuştur. Bu da anket cevaplayıcıları açısından, iç denetim birimlerinin henüz KRY temelli çalışmadığı fakat bu yönde işletmeler tarafından hazırlıkların tamamlanmak üzere olduğunu göstermektedir.

4.5.7. Ankete İlişkin Genel Değerlendirme

Anket sonuçları genel olarak Türkiye'de iç denetimde risk yönetimi temelli çalışmaya yönelik adımların atıldığı fakat gerek bütün risklerin dikkate alınması gerekse risk yönetiminin etkinlik değerlendirilmesi başta olmak üzere KRY aşamalarında iç denetim birimlerinin etkinliklerinin düşük olduğunu göstermektedir.



Şekil 12: Türkiye'de İç Denetim

Kaynak: PricewaterhouseCoopers, **Internal Audit 2012,** USA, 2007, s. 6'dan alınarak Türkiye verilerine göre uyarlanmıştır.

Şeklin yatay ekseninde kurumsal risk yönetimi olgunluk seviyesi gösterilirken dikey ekseninde ise denetimin odak noktası yer almaktadır.

Yukarıdaki şekil başta Tablo 34, 39, 40 ve 44 olmak üzere anket değerlendirmeleri sonucu elde edilen verileri temsil etmektedir. İç denetimin risk yönetimi verileri ile çalışması kuşkusuz risk yönetimi olgunluk seviyesi ile ilgilidir. Bu süreçte; işletme iç denetim biriminin katkısı ise, risk yönetimi olgunluk seviyesine ve üst yönetimin iç denetim birimine biçmiş olduğu role göre farklılaşabilmektedir.

4.6. MÜLAKAT ÇALIŞMASI

Faaliyet raporu ve kurumsal yönetim uyumluluk raporu incelemelerinin ve anket sonuçlarının irdelenmesinin ardından önceki değerlendirmelerde tespiti mümkün olmayan alanlar için, denetim evreni ve risklerle ilişkisi gibi, mülakat çalışması tasarlanmıştır. Diğer bir ifadeyle mülakat çalışmasına derinlemesine bilgiye ulaşmak için başvurulmuştur. Çünkü rapor incelemeleri ve anket çalışmaları sonucunda ulaşılan bilgiler yüzeysel ve sınırlıdır.

Mülakat çalışması, araştırma alanına giren örnekler arasından, genel olarak araştırma konusunu temsil etme özelliği olan az sayıdaki örneğin sistematik olarak incelenmesidir[431].

Mülakat çalışmasının içeriği, anket sonuçlarına göre tasarlanmıştır. Ayrıca mülakat çalışması yapılacak kurumların belirlenmesi sürecinde faaliyette bulundukları sektörü temsil kabiliyetlerinin bulunup bulunmadığına dikkat edilmiştir. Bu çalışmada, farklı sektörlerde faaliyet gösteren işletmeler üzerinde mülakatlar yapılmış ve standart soru setleri kullanılmıştır.

4.6.1. Mülakat Çalışmasının Kapsamı ve Sınırları

Uygulama kısmının ilk iki adımı olan raporların incelenmesi ve anket değerlendirmeleri sonucunda mülakat çalışması tasarlanmış ve yapılmıştır. Bu çerçevede çalışmanın genel amaçları doğrultusunda mülakat çalışması yapılacak kurumlar; reel sektörden bir işletme, bankacılık sektöründen bir işletme ve bir de iç

[431] Malhotra Naresh K., **Marketing Research,** USA, Pearson Prentice Hall, 2007, s. 42.

denetim danışmanlık hizmetleri veren bir bağımsız denetim firması şeklinde belirlenmiştir.

Mülakat çalışması; ilgili bankanın CEO'su, reel sektör ağırlıklı faaliyet gösteren holding işletmesinin iç denetim grup başkanı ve iç denetim danışmanlık hizmeti veren bağımsız denetim firmasının kıdemli iç denetim müdürü ile yapılmıştır.

4.6.2. Mülakat Çalışması Soruları

Mülakat çalışması sorularının hazırlanması sürecinde uygulama kısmının ilk iki adımı rapor incelemeleri ve anket çalışması değerlendirmelerinden ve "Internal Control from a Risk Based Perspective[432]", "Enterprise Risk Management: Pulling it all Together" ile "Risk and Management Accounting" isimli çalışmaların mülakat çalışması kısımlarından yararlanılmıştır.

Mülakat çalışması soruları, kurumsal risk yönetimi sürecinin aşamaları arasında yer alan iç kontrol ortamı ve risk tanımlama aşamalarından oluşmaktadır. Bunun gerekçesi, Türkiye'nin genel olarak KRY temelli denetimin başlangıç aşamalarında olması şeklinde ifade edilebilir. Mülakat sürecinde Ek II'de yer alan standart soru setleri kullanılmıştır.

4.6.3. Mülakat Çalışması Değerlendirmeleri

4.6.3.1. Bankacılık Sektörü Mülakat Bulgularının Değerlendirilmesi

Bankacılık sektörünün lider kurumları arasında yer alan ve 2007 yılı aktif büyüklüğü itibariyle ilk dörtte yer alan Banka CEO'su düzeyinde gerçekleştirilen bu mülakat çalışması ile sektör iç denetim uygulamaları hakkında ayrıntılı bilgiye ulaşılmaya çalışılmıştır.

Mülakat çalışmasına konu olan Banka, aynı zamanda Türkiye'nin önde gelen bir holdingine bağlıdır ve bu kapsamda Banka, kendi bünyesindeki iç denetim biriminin yanısıra bir de holding iç denetim biriminin denetimi altındadır. Holding iç denetim birimi soruşturma bölümü, bilgi teknolojileri denetimi, kredi riski denetim

[432] International Federation of Accountants, **Internal Control from a Risk Based Perspective,** USA, 2007, ss. 10-34.

bölümü, piyasa riski denetimi ve operasyonel risk denetim bölümlerinden oluşmaktadır.

Görüşme esnasında elde edilen bulgular iç kontrol ortamı ve risk tanımlama süreci şeklinde iki kısımda değerlendirilmiştir.

A. İç kontrol Ortamı

Bankacılık sektörü tarafından kullanılan ve bütün dünyada kabul gören BASEL II yaklaşımı çerçevesinde risk yönetim sistemi bankada konumlandırılmıştır. Buna ilave olarak yine Bankacılık mevzuatının öngörüleri kapsamında risk yönetimi ve iç denetim birimleri konumlandırılmıştır. BASEL II'nin tercih edilmesinde yasal bir zorunluluk olan BDDK'nın yol haritası büyük etkendir.

Banka İç Denetim Birimi, BDDK'nın hazırlamış olduğu "Bankaların İç Sistemleri Hakkında Yönetmelik[433]" çerçevesinde görevini yerine getirmektedir. Banka ve iştiraklerinin taşımakta olduğu riskler bir risk matrisi aracılığıyla değerlendirilmekte, Banka üst yönetimi, iç kontrol birimi ve risk yönetimi birimlerinin risklerin azaltılması yönündeki kontrol faaliyetleri de dikkate alınarak net risk düzeyleri ortaya çıkarılmaktadır. Devamında iç denetim biriminin kapasitesi de dikkate alınarak risk matrisinin sonucunda ortaya çıkan sayısal risk sonuçlarına göre denetimi yapılacak banka departmanlarının/iştiraklerinin/şubelerinin öncelik sırası tespit edilmekte ve yıllık denetim planı oluşturulmaktadır. Bu anlamda İç Denetim Birimi Bankanın Kurumsal Risk Yönetimi sürecindeki her noktada kredi, piyasa ve operasyonel risklerin yıllık denetimini yerine getirmektedir.

Ayrıca Banka iç denetim birimi 2007 yılı içinde bağımsız denetim şirketi tarafından dış denetime tabi tutulmuş ve Uluslararası Denetim Standartlarına uygun olarak denetimlerini yerine getirdiğine dair "uygunluk sertifikası" ile belgelendirilmiştir.

İç denetim birimi banka içindeki rolünü, bağımsız, tarafsız, objektif ve gerekli bilgi ve belgelere erişim için verilen yetkilendirilmeler çerçevesinde yürütür. İç denetim birimi icrai görevi bulunmayan Yönetim Kurulu üyeleri arasından seçilen denetim komitesi aracılığıyla Yönetim Kurulu'na bağlı olarak ve onun adına

[433] Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankaların İç Sistemleri Hakkında Yönetmelik",** 01.11.2006 tarih ve 26333 sayılı Resmi Gazete.

denetimlerini sürdürmektedir. Bu durum iç denetim biriminin bağımsızlığı açısından son derece önemlidir.

İç denetim ve risk yönetim birimleri Yönetim Kurulu'na bağlı olarak görevlerini yerine getirmekle birlikte birbirlerinden farklı olarak değerlendirilmektedir. Ancak Banka genelinde riskleri minimize etmek amacıyla her iki birim arasında bilgi paylaşımı olmaktadır ve iç denetim birimi ilgili yönetmelik gereğince risk yönetimi ve iç kontrol Birimlerini yıllık plan dahilinde denetlemektedir.

Banka, iç denetim birimi açısından danışmanlık ve güvence hizmetleri arasındaki hassas dengeyi korumak çok önemlidir. Bu kapsamda iç denetim birimi mevcut/olası riskleri minimize etmek amacıyla gerekli tedbirlerin alınmasını teminen bankadaki diğer iş birimlerine danışmanlık ve güvence hususlarında görüş bildirmektedir.

B. Risk Tanımlama Süreci

Bankanın karşılaştığı riskler kredi, operasyon ve piyasa riskleri açılarından risk matrisi aracılığıyla sayısal skorlamaya tabi tutulmakta, skorlama yapılırken kontrol risk öz değerleme, geçmiş dönem denetim sonuçları, son denetimden bu yana geçen süre gibi faktörler dikkate alınarak tanımlanmaktadırlar.

Risklerin tanımlanması sürecinde karşılaşılan zorlukların başlıcası, riskleri sayısal bir değer vererek ölçme olarak ifade edilmiştir. Banka subjektif sonuçlardan kaçınmak için risk matrisi içinde sayısal değerleri kullanmaktadır. Diğer yandan risklerin sürekli değişmesi ise sorun değildir. Çünkü risk odaklı denetim planı çerçevesinde denetimi yapılacak banka birimlerinin sayısal notlarının sonuçlarına bakılarak öncelik sırasına göre yıllık denetim planı gerçekleştirilmektedir.

Risk ve denetim evreni bankada; şubeler ve Banka birimlerinin tamamı olarak kabul edilmektedir. Buna göre her birimin bankacılık faaliyeti ayrı ayrı sayısal olarak risk matrisinde değerlendirmeye tabi tutulmaktadır. Bankadaki her birimin faaliyetlerinin kredi, operasyonel ve piyasa risk seviyeleri, son denetimden beri geçen süre, dış mevzuata uygunluk, itibar riski, dış denetim firmasının değerlendirmesi ve son denetim raporu notu ele alınan başlıca risk faktörleridir.

Mülakat esnasında denetim evreninin tüm risk türlerini; kredi, operasyonel ve piyasa riskini içerdiği bilgisine ulaşılmıştır. Fakat Banka risk ve denetim evreninin kaç adet riskten/riskli faaliyetten oluştuğu hakkında kesin bir bilgiye görüşme esnasında ulaşılamamış ve bankacılık sırları kapsamında bilgi verilmesi uygun görülmemiştir.

Bankacılık sektörü ve diğer işletmeler açısından önemli bir sorun da; denetim evrenine alınmayan risklerden dolayı işletmenin zarara uğrama ihtimali ve bu bağlamada denetçinin üstlendiği/üstlenmesi gereken sorumluluktur. Bu bağlamda Banka'da yıllık plan taslak olarak hazırlandıktan sonra denetim komitesi aracılığıyla Yönetim Kurulu onayına sunulduğu ve onay sonrası BDDK'ya gönderilmektedir. Bu kapsamda risklerden dolayı işletmenin zarar uğraması halinde sorumluluk üst yönetimdedir.

Banka'da risk kayıtlamalarına ilişkin sorumluluk en üst düzeyde Yönetim Kurulu'na aittir, risk ölçümlemesi ve raporlanması ise risk yönetimi departmanı tarafından yapılmaktadır. Banka risk alma istekliliği sınırı üst yönetim tarafından belirlenmekte ve iç denetçinin ancak yeni süreçler/gelen danışmanlık talepleri esnasında riskin minimize edilmesi yönünde görüş bildirme mükellefiyeti bulunmaktadır.

Risk tanımlama sürecinde iç denetçinin ve denetim komitesinin görevi; Yönetim Kurulu'nu Banka'nın karşılaştığı riskler hakkında en iyi şekilde bilgilendirmek olduğundan dolayı çok önemlidir. Yönetim Kurulu seviyesinde doğru kararların alınmasında etkin rol oynarlar" şeklinde açıklanmıştır.

4.6.3.2. Reel Sektör Mülakat Bulgularının Değerlendirilmesi

Mülakat yapılan işletme, Güney Avrasya ve Orta Doğu'yu kapsayan bir alanda içecek sektöründe faaliyet göstermektedir ve ortaklık yapısı itibariyle Türkiye'nin önde gelen holdinglerinden birine bağlıdır. İşletme İç Denetim Müdürü düzeyinde gerçekleştirilen mülakat ile reel sektör iç denetim uygulamaları hakkında ayrıntılı bilgilere ulaşılmaya çalışılmıştır.

Mülakat çalışmasına konu işletmede İç Denetim Müdürü aynı zamanda Risk Yönetim faaliyetlerini de koordine etmektedir ve bu iki fonksiyonu yürüten ekip ayrı kişilerden oluşmaktadır. Departmanda güvence esaslı çalışan bölüm denetim

faaliyetini yürütürken danışmanlık esaslı çalışan bölümse risk yönetimi faaliyetlerini yürütmektedir.

İşletme iç denetim biriminin amacı, yönetim tarafından hazırlanarak ilan edilen risk yönetimi ile denetim ve yönetim süreçleri ağının yeterli olup olmadığını belirlemektir. Ayrıca aşağıda ifade edilen faaliyetlerde iç denetim biriminin amaçları arasında yer alır. Bunlar:

- Risklerin zamanında belirlenmesi ve kontrol edilmesi,
- Gerektiği durumlarda çeşitli yönetim kademeleriyle etkileşimin sağlanması,
- Önemli nitelikteki mali, yönetsel ve işletme bilgilerinin doğru, güvenilir ve zamanına uygun olması,
- Çalışanların kurum "Etik Politikasına" uygun hareket etmesi,
- Kaynakların ekonomik şekilde elde edilmesi, verimli kullanılması ve yeterli ölçüde korunması,
- Faaliyetlerin ve programların, saptanmış olan hedeflere ve amaçlara uygun olması ve faaliyetlerin veya programların planlandığı şekilde gerçekleştirilip gerçekleştirilmediğinin kontrol edilmesi,
- Şirketin denetim sürecinde, kalitenin ve sürekli ilerlemenin teşvik edilmesi,
- Şirketi etkileyen önemli yasal veya idari sorunların zamanında tespit edilmesi ve çözülmesidir.

Görüşme esnasında elde edilen bulgular İç Kontrol Ortamı ve Risk Tanımlama Süreci şeklinde iki kısımda değerlendirilmiştir.

A. İç kontrol Ortamı

İşletme uygulamaları daha çok COSO KRY çerçevesinin kullanıldığını göstermektedir. Fakat uygulamada özellikle BASEL veya COSO şeklinde bir ayrımda bulunulmadığı anlaşılmaktadır.

Riski yönetimi ve iç denetim birimini yürüten ekip ayrı fakat organizasyon düzeyinde sorumluluk tek kişide toplanmıştır. Bu anlamda işletmede risk yönetim birimi risk yönetimi sisteminin işleyişini gerçekleştirmekte iç denetim birimi de risk yönetim sistemine ait rutin denetim faaliyetlerini üstlenmektedir.

İşletmede iç kontroller ve iç denetim çok temel bir risk yönetim faaliyeti olarak algılanmaktadır ve her iki sistem birbirlerini destekler tarzda konumlandırılmıştır.

Risk yönetimi faaliyetlerini yürüten ekiple iç denetim faaliyetlerini yürüten ekiplerin ayrı olması bağımsızlık konusunda İç Denetim Müdürü'nü rahatlatmaktadır. Aynı zamanda İç Denetim Müdürü'nün risk yönetimi ve iç denetim birimi faaliyetleri ile ilgilenirken farklı tutumlar takınması bağımsız hareket etmeyi mümkün hale getirmektedir.

B. Risk Tanımlama Süreci

İşletme yaklaşık 10 yıldan beri risk odaklı denetimi uygulamaktadır. Ayrıca, hem makro hem de mikro bazda işletme operasyonel riskleri değerlendirilmekte ve bu riskleri idare etmeye yönelik kontroller test edilmektedir.

İşletmede, makro düzeyde (daha çok risk yönetimi faaliyeti) gerçekleştirilen risk tanımlama sürecinde çalıştaylar mikro düzeyde (iç denetimin bir aşaması da olan risk değerleme faaliyeti); gerçekleştirilen risk tanımlama sürecinde ise öz değerleme yöntemi kullanılmaktadır. Tanımlanan riskler yılda iki kez de gözden geçirilmekte ve böylelikle risklerin güncel kalmaları sağlanmaktadır.

Risk tanımlama sürecine katılan yöneticiler de dahil çalışanların ortak bir terminolojiye sahip olmamaları bu süreçte karşılaşılan en büyük zorluk olarak dikkatleri çekmektedir. Bu zorluk da işletmenin tecrübeleri ve geçmiş yıllarda oluşturulan risk tanımlarından elde edilen verilerle ortadan kaldırılmaktadır. İşletmede, 24 ana risk kategorisinde yaklaşık 174 adet risk tanımlanmıştır.

İşletmenin uygulamalarında denetim evreninin kaç adet riskli faaliyetten oluştuğu konusunda bir bilgiye ulaşılamamıştır. Ayrıca görüşmede Türkiye'de, denetim evrenlerinin ne kadar faaliyetten oluştuğuna ilişkin bir bilgiye ulaşılamamıştır. Ayrıca bu konununda pek dikkatleri çekmediği anlaşılmaktadır.

Mülakat çalışmalarından anlaşıldığı üzere sektörel farklılıklar, işletmelerin ihtiyaçları ve üst yönetimin talepleri denetim evrenine dahil edilecek faaliyetleri etkilemekte ve sonuç olarak da farklı işletmelerin hazırlamış oldukları denetim evrenlerinde değişik özellikler gösterdiği anlaşılmaktadır. Örneğin bazı işletmelerde

denetim evreni bölgeler temelinde ayrımlanıp faaliyetler sıralanırken bazı işletmelerde de departman temelli bir ayrıma gidildiği gözlemlenmiştir.

İşletme iç denetim birimi tarafından hazırlanan denetim planı denetim komitesinin incelemesi ve onayının ardından denetim faaliyetlerinde dikkate alınmaktadır. Denetim evreninin ise denetim komitesinin onayına sunulmadığı anlaşılmıştır.

İşletmede risk yönetimine ve risk alma istekliliklerinin belirlenmesine ilişkin sorumluluk, denetim komitesi ve yönetim kurulundadır. Risk alma istekliliklerinin belirlenmesinde iç denetim birimi gerekli eğitim ve danışmanlık ihtiyaçlarını karşılamaktadır.

Sonuç olarak risk yönetimi sürecinde denetim komitesinin ve yönetim kurulunun zamanlı ve doğru kararlar alabilmeleri iç denetim biriminin ne kadar etkin çalıştığı ile direkt ilişkilidir.

4.6.3.3. Bağımsız Denetim Firması Mülakat Bulgularının Değerlendirilmesi

Global ölçekte faaliyet gösteren bir bağımsız denetim firması olan ve başta finans sektörü olmak üzere reel sektörden de pek çok işletmeye denetim, vergi ve danışmanlık hizmeti veren kuruluşun Türkiye yetkilileri ile mülakat yapılmıştır.

Firma, müşterilerinin risklerini yönetmelerine ve bu sayede onların ana faaliyet alanlarına yönelmelerine yardımcı olmaktadır. Bu çerçevede firma tarafından; risk değerlemeleri, risk çeşitleri, hazine, bilgi sistemleri ve tedarik gibi alanlardaki kontrollerin incelenmesinde danışmanlık hizmetleri verilmektedir.

BASEL II kriterleri çerçevesinde risk yönetimi danışmanlık hizmetleri veren firma; işletmelerde iç denetim ve risk yönetimi faaliyetlerinin bütünleştirilmesi çalışmalarını ağırlıklı olarak yürütmektedir.

Mülakat Ek II'de verilen sorular çerçevesinde gerçekleştirilmiştir. Görüşme esnasında elde edilen bulgular iç kontrol ortamı ve risk tanımlama süreci şeklinde iki kısımda değerlendirilmiştir.

A. İç kontrol Ortamı

Risk Yönetimi sürecinde danışmanlık hizmeti verilen sektöre ve hizmet verilen kurumun tabi olduğu yasal mevzuata göre uygulanan yöntemde farklılıklar ortaya çıkabilmektedir. Bununla birlikte, genel olarak reel sektör risk yönetiminde COSO ağırlıklı olarak yer alırken, finans sektörü için BASEL ön plana çıkmaktadır.

Kullanılan rehber çerçeve seçimini genellikle; hizmet verilen kurumların yasal mevzuata uyum yükümlülüklerinin, kontrol ortamının ve genel olarak kurumun kendi ihtiyaçlarının etkilediği gözlemlenmiştir. Risk yönetimi hassas ölçüm ve modelleme tekniklerine göre yapıldığından, bir kurum için uygun olan bir risk yönetim stratejisi ve modeli, başka bir kurum için uygun olmaması normaldir. Dolayısıyla, risk yönetiminde tercih edilen çerçeve için standart kurallar koymak uygun bir yaklaşım olmamaktadır. Zamana ve duruma göre değişen dinamik bir yaklaşım yardımıyla risk yönetimi uygulanmaktadır.

Günümüzde iç denetim, sürekli değişen iş ortamında zorlu olmakla birlikte, aynı zamanda fırsatlarla dolu bir konumdadır. Katma değer yaratan bir iç denetim yaklaşımı için, iç denetimin değişen rolünün iyi anlaşılması, önceliklerinin belirlenmesi ve güçlü olduğu alanlarda faaliyetlerini devam ettirmesi hızlı değişen piyasa koşullarına uyum açısından önem taşımaktadır. Türkiye'de iç denetim kurumsal risk yönetiminin etkin bir şekilde uygulanmasında önemli role sahiptir. Ancak, Türkiye de kurumsal risk yönetim kültürü firmalarda henüz tam olarak benimsenmediği için Türkiye'deki iç denetim uygulamaları uluslararası uygulamalarla kıyaslandığında, hala tamamlanması gereken önemli eksiklikler vardır.

Son zamanlarda iç denetim anlayışında ve organizasyon içerisinde üstlendiği rollerde bir değişim gözlenmektedir. Buna göre, iç denetim artık "bilgi veren" değil, "yorum katan" konumundadır. Yeni iç denetim yaklaşımında, bilgi analiz ve sentez edilerek üst yönetime sunulmaktadır. Bu yolla yöneticiler iş ortamındaki gelişen ve değişen eğilimler, fırsatlar, tehditler ve riskler konusunda daha etkin kararlar alabilmektedir. Günümüzde Yönetim Kurulu üyeleri ve Denetim Komitesi üyeleri artık İç Denetim Bölümünden sadece münferit konularda yazılmış raporlamalar yapması yerine, "gerçek zamanlı-anlık" olarak kontrol ortamı hakkında geri bildirimleri talep etmektedir. Özellikle üst yönetim, kontrol ortamının güvenilirliği

konusunda bir kanaate varırken, İç Denetim Bölümünün görüşlerini dikkate alarak karar vermektedir.

İç denetim ideal olarak organizasyonun Kurumsal Risk Yönetimi'ne katkı sağlarken, iş süreçlerine ve bu süreçlerin sorumlusu konumundaki çalışanlara da danışmanlık rolünü üstlenmektedir.

Bununla birlikte, İç Denetçilerin risklerin tanımı ve kontrol mekanizmaları konusunda organizasyon genelinde "ortak dil" oluşturmaları önemli bir başarı faktörü olarak değerlendirilmektedir. Riskin olma olasılığı ve etkilerinin tüm çalışanlar tarafından doğru anlaşılması kontrol maliyetlerini de daha etkin hale getirecektir. Bu yaklaşımın başarılı olabilmesi için, iç denetimin bilgi teknoloji sistemleri ve veri madenciliği araçları ile desteklenmesi gereklidir.

Genel olarak bakıldığında, iç denetim ve risk yönetimi birbirini tamamlayan unsurlardır. Bununla birlikte, danışmanlık hizmeti verilen kurumlarda kurum kültürüne ve faaliyet gösterdiği sektörel gelişmelere bağlı olarak farklı bakış açıları ile karşılaşılmaktadır.

Genel olarak bağımsız denetim firması, iç denetim danışmanlık hizmeti verdiği kurumlara bağımsız denetim hizmeti vermeme yönünde bir tutum izlemektedir. Tersi durumda yani bağımsız denetim hizmeti verdiği kurumlara da iç denetim danışmanlık hizmeti vermemektedir.

B. Risk Tanımlama Süreci

Risk tanımlama süreci kuruma ve sektöre göre değişkenlik gösteren bir uygulamadır. Bununla birlikte, son dönemde yaygın olarak kurumlar tarafından tercih edilen çalıştay aracılığı ile risklerin tanımlanması yöntemi gözlemlenmiştir.

Risk stokastik özelliğe sahip olduğundan, modellemek ve ölçmek için öncelikle iyi tanımlanması gerekmektedir. Riskin temel unsurlarının etkisinin ve ortaya çıkma olasılığının değişken olduğu unutulmamalıdır. Bu nedenle risklerin dinamik piyasa koşullarında tam ve zamanında tanımlanması büyük zorluklar içermektedir.

KRY çerçevesinin en temel adımı sayılan risk tanımlama denetim evreni ile yakın ilişki içindedir. İç denetim danışmanlık hizmetlerini de yürüten firma; denetim evreninin oluşturulmasında dikkate alınması gereken dört temel perspektifte toplam

17 unsurun önem taşıdığını ve genelde bu çerçeveye uygun hareket ettiklerini belirtmişlerdir. Bunlar aşağıdaki gibidir[434]:

I. Risk Yönetimi

1. Risk yönetiminin görev ve sorumlulukları: Mevcut yapının, risk yönetimi çerçevesindeki işlevlerin ve sorumlulukların tanımlanması.

2. Risk stratejisi: Risk yönetimi hedeflerinin ve iş entegrasyonunun belirlenmesi.

3. İş süreçlerine entegre edilmesi: Risk yönetiminin, kurumsal yönetim ve iş süreçleriyle entegrasyon derecesi.

4. İç Kontrol: İç kontroller süreç hedefleri için makul ölçüde güvence sağlamalıdır.

5. "Savunmanın Üçüncü Hattı": Kurum içi gözetim işlevi (Risk komitesi, iç ve dış denetim gibi)

II. İnsan Kaynağı

1. Uygunluk: Risk yönetimi ile ilgili sorumluluk alan çalışanların nitelikleri.

2. Görev tanımı: Görev ve sorumlulukların belirlenmesi.

3. Eğitim ve Gelişim: Çalışanların tecrübesi ve kişisel özellikleri.

4. Kültür: Risk yönetiminin şirket kültürünün bir parçası olması.

III. Altyapı

1. Modelleme: Risk yönetimi için geçerli modellemeler.

2. İletişim Yönetimi: Çalışılacak ve analiz edilecek bilgilerin uygun iletişim kanallarından temin edilmesi.

3. Politika ve Prosedürler: Geçerli kuralları kapsayan risk yönetimi çerçevesinin belirlenmesi.

4. Dış Kaynak Kullanımı: Dış kaynak kullanımında, ortak girişimlerde ve bağlı ortaklıklarda risk yönetimi.

[434] KPMG, KPMG Metodoloji 2008.

IV. Riskin Raporlanması

1. Kullanıcı: Risk yönetim fonksiyonundan değişik iç ve dış ortaklar bilgi beklemektedirler.

2. İçerik: Risk raporlamasında sunulan risk yönetim bilgilerinin tipleri.

3. Frekans: Risk raporlamasının sıklığının belirlenmesi.

4. Entegrasyon: Risk raporlamalarının şirketin raporlama süreçlerine ve yönetim raporlamalarına entegrasyonu.

Ayrıntılı ele alınan risk yönetimi, insan kaynağı, altyapı ve riskin raporlanması süreçlerini içeren denetim evreni oluşturulurken üst yönetimin onayı alınmaktadır. Burada aksayan bir durum olması halinde, danışmanlık hizmeti verilen kurum bu hususta bilgilendirilerek uygun öneriler yapılmaktadır.

Genel olarak, makro düzeyde risk ve denetim evreni konuları kurumların ilgili yönetim birimleri tarafından hazırlanarak yönetim kurulu onayı ile uygulanmaya başlanmaktadır. Makro düzeyde riskleri tanımlamaktan sorumlu olan personelin güncel literatüre ve gelişmelere tam olarak hâkim olamaması halinde, sorunlar ortaya çıkabilir. Bu durum danışmanlık hizmeti sunulan kurumda harcanan çalışma adam/gün süresinde artışa ve daha fazla örneklem üzerinde denetim yapılmasına yol açmaktadır. Aynı zamanda maliyetlerin yükselmesi anlamına da gelmektedir.

Danışmanlık hizmeti verilen kurumlarda risk kayıtlaması risk yönetiminden sorumlu icracı olan yönetim birimleri tarafından yetkilendirilen personel aracılığıyla yapılmaktadır. En üst düzeyde sorumluluk verilen makam zaman zaman değişmekle birlikte, genellikle CEO, Genel Müdür Yardımcısı veya Direktörlere verildiği gözlenmektedir. Bu hususta yasal düzenleme olduğu takdirde, söz konusu düzenlemelere (Bankalar Kanunu, SPK Mevzuatı vb.) paralel uygulamalarla karşılaşılmaktadır.

Risk alma sınırının yönetim kurulu, CEO veya ilgili limitler dahilinde genel müdür yardımcıları tarafından belirlendiği gözlenmektedir. İç denetim riskleri sürekli izleyerek değişen koşullara uyum sağlama ve tedbir alınması konusunda üst yönetime tavsiyelerde bulunmaktadır. İç denetimin icra yükümlülüğü olmadığından,

sorumluluğu yönetimi muhtemel riskler konusunda bilgilendirmekten ibarettir. Risklerin tespitinde ve denetiminde ise makul güvence sağlama görevi vardır.

İç denetim ile ilgili paydaşların beklentisi arttıkça, iç denetimin kaynaklarını ve kapasitesini optimum düzeyde kullanma zorunluluğu ve önceliklerini risk odaklı bir şekilde belirleme ihtiyacı ortaya çıkmaktadır. Hızla değişen iş dünyasında oldukça dinamik bir risk ortamı oluştuğundan dolayı, iç denetimin eskisinden daha fazla risk odaklı olmaya ve risk odaklı bir denetim anlayışıyla paydaşların beklentilerini karşılamaya çalışması gerekmektedir. Dolayısıyla, risk yönetim sürecinde tüm riskler olasılık ve etkileri dikkate alınarak değerlendirilmektedir.

Genel olarak iç denetimin ve denetim komitesinin kurum içerisinde üstlendiği önemli sorumluluklar, mülakat esnasında bağımsız denetim firması yetkilisi tarafından şu şekilde ifade edilmiştir:

- Bütünleşik güvence modelini uygulayarak yönetim kurulunu, denetim komitesini ve çok çeşitli paydaşlarının beklentilerini karşılayarak organizasyona fayda sağlamak ve bu yolla lider olmak,
- Organizasyona katma değer sağlamanın yanısıra, organizasyonun kontrol altyapısının geliştirilmesini ve kontrol ortamının iyileştirilmesini sağlamak,
- İç denetimin geliştirdiği yöntem ve teknikler aracılığıyla organizasyon genelinde risk bakış açısının uyumlaştırılmasını sağlamak ve güvence faaliyetlerini başarıyla uygulamak,
- Organizasyon genelinde kullanılabilecek rapor formatları ve süreçler geliştirmek ve üst yönetimin, yönetim kurulunun ve denetim komitesinin kontrol ortamına olan bakış açısının uyumlaştırılmasını sağlamak,
- İşe alımlarda sadece iç denetim alanındaki üstün yetenek ve tecrübeye göre değil, aynı zamanda analitik düşünme yeteneğine sahip iş ortamındaki gelişmeleri yorumlayarak aktarabilecek personelin iç denetim alanında işe alınması ve istihdam edilmesini sağlamak.

SONUÇ VE ÖNERİLER

Başta küreselleşme olmak üzere ekonomik faktörlerdeki ve teknolojideki gelişmeler, işletmelerin değişen organizasyon yapıları ve artan sermaye birikimleri işletmelerin faaliyetlerine ilişkin talep edilen bilginin niteliğinin ve derinliğinin değişmesine neden olmuştur. İşletmelerin faaliyet sonuçları ile ilgilenen tarafların farklılaşması ve bilginin güncel, zamanlı ve doğru olması yönündeki beklentiler denetim mesleğinde yaşanan değişmeleri özetlemektedir.

Denetimin geleneksel çalışma alanına, karar alıcıların ihtiyaç duyduğu bilginin niteliğindeki değişmelerden kaynaklanan diğer fonksiyonların da eklenmesi ile birlikte denetim; hata odaklı yaklaşımdan risk yönetimi temelli yaklaşıma, gelenekseli terk etmeden, zenginleşerek dönüşmüştür.

Yaşanan gelişmeler organizasyon yapılarına yansımış ve denetim komiteleri ağırlığı bağımsız üyelerden oluşmak koşuluyla uygulamada kendine yer bulmuştur. Organizasyon yapılarındaki anılan değişmeler bir on yıl öncesinde rastlanması pek sık olmayan sorumluluk alanlarını ortaya çıkarmıştır.

Denetim komitelerinin bağımsız denetim, iç denetim ve risk yönetimi alanlarında çeşitli görevleri ve sorumlulukları bulunmaktadır. Sözkonusu bu birimlerin kendi aralarında çıkar çatışması olmaksızın etkin bir şekilde faaliyetlerini sürdürebilmeleri kurumsal yönetim ilkelerinin desteğiyle mümkün olmaktadır.

Risk yönetimi ve kurumsal yönetim ilkeleri çerçevesinde yaşanan bu değişikliklere paralel olarak COSO tarafından 1992 yılında iç kontrol ve 2004 yılında KRY çerçevelerinin yayınlanması, uygulamada asgari şartların oluşması yönünde olumlu katkılarda bulunmuştur.

Özellikle KRY çerçevesi ile birlikte risk yönetimine ait terminolojinin oluşması daha kolay olmuştur. Ayrıca KRY çerçevesinin, iç kontrol çerçevesinin "risk değerleme" aşamasına dayanması ve risk yönetiminin temelinde kontrollerin

bulunduğu gerçeği, bu süreçte iç denetim biriminin katkısının ne olabileceği konusunu ve denetimde kullanılmak üzere risk yönetimi sisteminden alınabilecek veri setlerini gündeme getirmiştir.

İç denetim faaliyetinin risk yönetimi sisteminden veri alması, geleneksel anlamdaki risk değerleme faaliyeti için olumlu katkıda bulunmakta ve denetime ayrılabilir kaynakların kritik alanlara aktarılmasını ve denetimin planlanmasını kolaylaştırmaktadır. Öte yandan iç denetim birimi, risk yönetimi faaliyetine yönelik güvence ve danışmanlık hizmetleri verebilmektedir. Verilecek hizmetin çeşitliliği başta kurum risk yönetimi olgunluğu olmak üzere üst yönetimin tutumu, denetim komitesinin istekleri ve iç denetim yönetmeliğis ile ilgilidir.

Risk yönetimi olgunluğunun ilk seviyesi olan "saf riskler" aşamasında denetimin kullanabileceği güvenilir herhangi bir veri bulunmamakta ve denetçi risk yönetimi sürecinde öncü-danışman rolü üstlenebilmektedir. Diğer yandan risk yönetimi olgunluğunun son seviyesi olarak kabul edilen "bütünleştirilmiş riskler" aşamasında denetçi güvenilir bir veri seti bulabilmekte ve sıklıkla bu aşamada denetim biriminden güvence hizmeti vermesi beklenmektedir.

Bilindiği üzere KRY çerçevesinin bileşenleri kontrol ortamı, hedeflerin belirlenmesi, olay tanımlama, risk değerleme, risk tutumu, kontrol faaliyetleri, bilgi ve iletişim ile izlemedir. KRY çerçevesi bileşenlerinden ilk beşi denetimde planlama ile, KRY çerçevesinin altıncı bileşeni denetimin yürütülmesi ile; KRY çerçevesinin son iki bileşeni ise denetimde raporlama ile paralel bir şekilde çalışmaktadır.

Denetimin planlama aşamasına kurum denetim stratejisi yön verir. Bu aşamada denetçi denetim evrenini hazırlar. Denetim evreninin hazırlanması sürecinde risk kayıtlamasından yararlanacak olan denetçi aynı zamanda bir risk yönetimi çıktısı olan risk matrisi (risk haritası) aracılığıyla da işletme risklerini denetim evrenine aktarma fırsatını yakalar. Üst yönetimin istekleri doğrultusunda belirlenen ve denetçi tarafından sağlanan güvence seviyesi, denetimin kapsamını etkilemektedir. Planlamanın son aşaması ise denetim komitesine ve üst yönetime planın sunulması ve varsa değişiklik isteklerinin dikkate alınarak plana son halinin verilmesidir.

Planlamadan sonraki aşama denetimin plana göre yürütülmesidir. Klasik anlamda denetim personelin görevlendirilmesi ile başlar ve denetim programına

uygun bir şekilde denetim testlerinin yürütülmesi ile bu aşama tamamlanır. Burada özellik gösteren durum, denetçinin risk yönetimi faaliyetlerinin izleme aşamasında görev alması halinde, sözkonusu alan hakkında uzmanlık seviyesinin yeterli olması gerekliliğidir.

Raporlama öncesinde denetçinin elde ettiği bulguları değerlendirmesi gerekmektedir. Geleneksel olarak denetim bulgularının değerlendirilmesinin yanısıra denetçi incelediği alandaki veya kurum genelindeki risk yönetimi olgunluğunu değerlendirir. Denetçi risk yönetimi olgunluk değerlendirmesini strateji, süreç, insan, teknoloji ve bilgi açılarından yapar.

Denetimin son aşaması raporlamadır. Geleneksel raporlamadan farklı olarak KRY temelli iç denetimde raporlama; önemli risklere, kontrol sorunlarına ve ilgili kontrol tavsiyelerine odaklanmaktadır. Risk değerlemelerinin yer alması gerektiği raporda risk yönetimi etkinliği ile risklerin önemlilik düzeyi ayrıca ele alınmalı ve gerekli tavsiyelerde bulunulmalıdır.

KRY çerçevesinin incelendiği ardından iç denetimle risk yönetiminin ortak çalışma alanlarının belirlendiği bu çalışmanın uygulama kısmı faaliyet ve kurumsal yönetim uyum raporlarının incelenmesi, anket ve mülakat çalışması şeklinde tasarlanmıştır.

İMKB'de hisse senetleri işlem gören 320 firmadan 232'sinin (% 72,5) raporu elde edilmiştir. Faaliyet ve kurumsal yönetim uyum raporlarının yayınlanma zorunluluğu bulunmasına rağmen yayınlanmaması, e-posta veya telefonla talep edilmesine rağmen ulaşılamaması sistemin ülke düzeyinde henüz tam oturmadığını bir başka ifadeyle rapordan beklentilerin tam anlamıyla gerçekleşmediğini göstermektedir.

Faaliyet raporu incelemeleri sonucunda İMKB'de hisse senetleri işlem gören firmalardan % 57'sinde iç kontrol birimin bulunduğu ve % 19'unda da uluslararası standartlara paralel bir şekilde fonksiyonel ve idari raporlama yapıldığı bilgisine ulaşılmıştır. Ayrıca raporlardan 16'sında ki bunların tamamı bankalara aittir, bağımsız denetçinin raporları incelediği ve görüş bildirdiği (tümü olumlu) anlaşılmaktadır.

Faaliyet ve kurumsal yönetim uyum raporu inceleme sonuçları dikkate alınarak anket soruları tasarlanmış ve posta aracılığıyla İMKB'de hisse senetleri işlem gören firmalara (320 firma) gönderilmiştir. Ankete yanıt veren firma sayısı 79 olum toplamın % 24,7'sidir.

Ankete cevap verenler özelinde yapılan değerlemede işletmelerin % 84,2'sinde iç denetim biriminin olduğu sonucuna ulaşılmıştır. İşletmeler hem maliyetlerden hem de uzmanlaşmadan dolayı bir takım hizmetleri işletme dışından sağlamaktadırlar. Dışarıdan alınan denetim destek hizmetlerinin yaklaşık % 60,4'ünü yeminli mali müşavirlik hizmetleri oluşturmakta bunu % 15,3 ile bilgi teknolojilerinin denetimi izlemektedir.

İşletmelerde iç denetim biriminin kime raporlama yaptığı bağımsızlık açısından çok önemlidir. Uluslararası uygulamada iç denetim birimi, fonksiyonel olarak denetim komitesi veya dengi bir yönetim birimine ve idari olarak da kurum başkanına raporlama yapmaktadır. Türkiye örneğinde ise raporlamanın % 39'unun Genel Müdüre veya CEO'ya, kalan % 61'inin ise Yönetim Kurulu Başkanı, Yönetim Kurulu Üyesi veya Denetim Komitesine yapıldığı bilgisine ulaşılmıştır. Bu durum idari ve fonksiyonel şeklinde bir ayrıma gidilmediğini göstermekte dolayısıyla iç denetim birimlerinin uluslararası normlara uygun bir şekilde bağımsız çalışmadıklarını gözler önüne sermektedir.

Bu çalışmanın temelini oluşturan ve iç denetim faaliyetlerinin odak noktasını tespit etmek için yöneltilen soruya verilen cevaplardan, iç denetim birimlerinin uygunluk denetimi (4,30 ortalama) ve faaliyet denetimine (4,14 ortalama) ağırlık verdikleri belirlenmiştir. Öte yandan KRY faaliyetleri (3,19 ortalama) ile bilgi teknolojilerinin denetimi (2,88 ortalama) sıralamada en sonda yer almaktadırlar. Buradan anlaşıldığı üzere Türkiye'de iç denetim henüz kontrol odaklı yürütülmektedir.

İç denetim biriminin risk yönetimi ile ilgili hangi ağırlıkta güvence ve danışmanlık hizmeti verdiği, KRY'nin hangi safhada olduğu ile ilgilidir. Ankete verilen cevaplardan anlaşıldığı üzere işletmelerin % 36,8'inde KRY tam olarak faal ve yine % 36,8'inde KRY süreci başlamış ama tam olarak faal değil sonuçlarına ulaşılmıştır. KRY sistemini tam olarak uygulayan işletmelerin sayısı arttıkça bu süreçte iç denetim biriminin hem güvence veya danışmanlık hizmeti verme rolü

artacak, hem de risk yönetimi sisteminin çıktıları denetçiler tarafından daha sık kullanılabilir hale gelecektir.

KRY sürecinde iç denetim biriminin ne kadar ve hangi aşamalarda etkin olduğunun belirlenmesi, iç denetçiler tarafından verilen güvence ve danışmanlık hizmetlerinin sınırlarının çizilmesine yardımcı olacaktır. İç denetim birimlerinin % 50 ile en çok KRY'nin raporlama ve izleme aşamasında, % 26,3 ile risklerin analizi ve değerlendirilmesi aşamasında ve % 22,6 ile risklerin tanımlanması aşamasında etkin oldukları belirlenmiştir. Bu aşamalardan raporlama ve izleme daha çok güvence hizmetleri kapsamında değerlendirilebilir, risklerin analizi ve değerlendirilmesi ile risklerin tanımlanması aşaması ise danışmanlık hizmetleri kapsamında değerlendirilebilir. Ayrıca risk tutumunun belirlenmesi aşamasında iç denetçilerin % 10,5 oranında etkili olmaları, uluslararası iç denetim standartlarına paralel bir uygulamadır. Çünkü risk tutumlarının belirlenmesi bir üst yönetim faaliyetidir ve iç denetçi bu süreçte danışmanlık hizmeti olarak kabul edilebilecek eğitim faaliyetlerini üstlenebilir.

İç denetim birimlerinin çalışma zamanı içinde risk yönetimi faaliyetlerine ayırdıkları süre çok önemlidir. Bunun tespiti için yöneltilen soruya verilen cevaplar; % 30,7 oranında cevaplayıcının zamanlarının % 26-50 aralığını risk yönetim faaliyetlerine ayırdıklarını göstermektedir. İlerleyen yıllarda KRY süreçlerini uygulayan işletmelerin artmasıyla beraber denetimin risk yönetim faaliyetlerine ayırdığı zamanda bir artış yaşanacaktır. Bununla beraber iç denetim birimleri bu sürecin daha çok risklerin tanımlanması, değerlendirilmesi, izlenmesi ve risk yönetiminin etkinliğinin raporlanması aşamalarında rol almalı fakat risk tutumlarının belirlenmesi ve risklerin yönetimi aşamalarında rol almamalıdırlar.

KRY sürecinde güvence veya danışmanlık hizmeti veren iç denetim birimleri, KRY sürecinin henüz oluşturulmadığı işletmelerin iç denetim birimlerine kıyasla denetimin planlanması aşamasında riskleri dikkate daha fazla almaktadırlar. Denetimin planlanma aşamasında dikkate alınan riskler; finansal riskler (% 89,4), operasyonel riskler (% 84,2), stratejik riskler (% 53,9), itibar riski (% 47,3), bilgi teknolojileri riski (% 47,3) ve son olarak düzenleme riski (% 34,2) şeklindedir.

İç denetimdeki odak noktada kontrollerden risk yönetimine doğru yaşanan kayma iç denetçilerin farklı yeteneklere sahip olmalarını gerektirmekte sonuç olarak

operasyonel riskler daha anlaşılır hale gelmektedir. Ayrıca işletmelerin stratejik hedeflerine ulaşmaları açısından kurumsal yönetimin ne kadar önemli olduğunun denetçiler tarafından anlaşılması mümkün olmaktadır.

Türkiye'de iç denetimin kontrol odaklı çalıştığına dair benzer sonuçlara; ankette son soru olarak tasarlanan ve denetim yaklaşımı, denetçinin rolü, denetimin odak noktası ve denetçinin niteliklerinin belirlenerek denetim kültürünün tespitinin hedeflendiği soru ile ulaşılmıştır. Yapılan incelemeler sonucunda; Türkiye'de denetimin henüz kontrol odaklı çalıştığı, fakat risk yönetimi temelli çalışması yönünde de adımlar atıldığı anlaşılmaktadır.

Rapor incelemeleri ve anket çalışmasında ulaşılamayan verilere ulaşabilmek ve ilk elden bilgi almak amacıyla mülakat çalışması yapılmıştır. Mülakat çalışması banka, reel sektör ve bağımsız denetim firması yetkilileriyle gerçekleştirilmiştir.

Banka yetkilileriyle yapılan mülakat çalışmasında BASEL kriterleri ve yasal mevzuatın yönlendirmesi ile risk yönetiminde bir hayli ilerleme kaydedildiği bilgisine ulaşılmıştır. Özellikle BASEL II uzlaşısının da uygulamada hayat bulmasıyla beraber ileri düzeyde risk ölçüm yöntemlerinin kullanılmaya başlanacağı ve özellikle operasyonel risklerin ölçümü ve yönetimi konusunda Dünya standartlarına ulaşılacağı kabul edilmektedir. Risk yönetimi sisteminin ileri düzeyde kullanıldığı Banka'da iç denetim birimi temel olarak mevzuat gereğince risk yönetimi sisteminin etkinlik değerlendirmesini yapmakta, izlemeleri gerçekleştirmekte ve raporlamaktadır. Ayrıca iç denetim birimi risk yönetimi sürecinde yeni süreçler veya üst yönetimin istediği danışmanlık alanlarında faaliyet göstermektedir.

Banka risk ve denetim evreninin oluşturulmasında kredi, operasyonel ve piyasa risk seviyeleri, son denetimden beri geçen süre, dış mevzuata uygunluk, itibar riski, dış denetim firmasının değerlendirmesi ve son denetim raporu notu dikkate alınmakta ve evrene son halini verilmektedir.

Banka iç denetim birimi Denetim Komitesi'ne karşı sorumlu olarak çalışmakta ve böylelikle iç denetim biriminin bağımsızlığı muhafaza edilmektedir. Amerika uygulamasında uzun yıllardır varolan Denetim Komitesi uygulaması muhasebe denetim skandallarının yaşanmasını engelleyememiştir. Denetim Komitesi'nin etkinliği temelde komite üyelerinin bağımsızlıkları, uzmanlık alanları

ve komite faaliyetlerine yeterli vakti ayırmaları ile ilgilidir. Türkiye uygulamasına ilişkin Denetim Komitesi yönetmelik ve raporlarının yayınlanmaması komitelerin etkinlik değerlendirmesinin yapılmasına imkân vermemektedir.

Reel sektörde faaliyet gösteren işletme seçiminde, iç denetim müdürünün aynı zamanda risk yönetim faaliyetlerinin koordinasyonundan da sorumlu olması kriterine öncelik verilmiş ve örneğe uygun bir işletme yetkilisiyle mülakat çalışması gerçekleştirilmiştir.

Sözkonusu işletmede; iç denetim birimi kendi içinde ikiye ayrılmıştır. Bir grup uzman risk yönetimi faaliyetlerini yürütürken diğer grup iç denetim faaliyetlerini yürütmektedir. Burada karşılaşılan en büyük zorluk veri paylaşımında çıkmaktadır. İç denetim elemanları genellikle risk yönetim sistemi hakkında fazla veri istemekte ve denetim müdürünü baskı altına almaya çalışmaktadırlar.

İşletmede risk tanımlama sürecinde çalıştaylar ve kontrol risk öz değerlendirme yöntemlerinin kullanıldığı belirlenmiştir. Ayrıca risk yönetimi sürecinde karşılaşılan en büyük zorluk, ortak bir risk terminolojisinin olmaması şeklinde ifade edilmiştir. Bu konuda iç denetim biriminin üst yönetim ve diğer çalışanlara eğitim desteği vermesi gerekmektedir.

Son mülakat, risk yönetimi alanında danışmanlık destek hizmetleri sağlayan bir bağımsız denetim firması yetkilileri gerçekleştirilmiştir. Denetim firması temelde bağımsız denetim hizmeti verdiği müşterileri ile danışmanlık hizmeti verdiği müşterileri arasında bir farklılaşmaya gitmektedir. Buna göre denetim hizmeti verdiği müşterisine danışmanlık hizmeti vermemekte tersi durumda da danışmanlık hizmeti verdiği müşterisine denetim hizmeti vermemektedir.

Denetim firması yetkililerinin izlenimlerine göre son yıllarda risk yönetimi desteğine ihtiyaç duyan firma sayısı artmıştır. Risk yönetimi alanında güvence ve danışmanlık hizmeti verilirken iç denetçi tarafından üstlenilmemesi gereken roller konusunda Uluslararası İç Denetim Standartlarına uygun hareket edilmektedir. Risk yönetimi özelinde danışmanlık hizmeti verilirken karşılaşılan en büyük zorluk, işletmelerde riskler ve yönetimi hakkında ortak bir dilin olmaması şeklinde açıklanmıştır.

Bu çalışmada ele alınan teorik çerçeve ile uygulamaya ilişkin verilerin ışığında iç denetim ve risk yönetim sistemine yönelik izleyen öneriler sıralanmıştır:

- ✓ SPK mevzuatı çerçevesinde halka açık olan işletmelerde Denetim Komitesi kurulması zorunluluğu bulunmasına rağmen iç denetim birimlerinin kurulması konusuda herhangi bir zorunluluk yoktur. İvedi bir şekilde, halka açık işletmeler başta olmak üzere SPK'ya tabi işletmeler ve belirlenecek ciro büyüklüklerinin üzrindeki işletmeler için iç denetim birimlerinin kurulması zorunlu hale getirilmelidir,
- ✓ İşletmelerde iç denetim birimleri kurulması zorunluluğunun yanı sıra; iç denetim birimleri için işletmeler iç denetim yönetmeliği hazırlamalı ve yayınlamalıdır,
    - Yönetmelikte üst yönetim ve denetim komitesinin risk yönetim sürecinde iç denetim biriminden beklentileri yer almalıdır,
    - Yönetmelikte özellikle iç denetim biriminin, KRY sürecinde vereceği güvence ve danışmanlık hizmetleri açıklanmalıdır,
    - Yönetmelikte iç denetim biriminin bağımsızlığının pekiştirilmesi için organizasyon içinde raporlama yapılması gereken yetkililer, denetim komitesi ve yönetim kurulu başkanı gibi, belirtilmelidir,
- ✓ Kurulma zorunluluğu olan Denetim Komiteleri için, işletmeler Denetim Komitesi yönetmeliği hazırlamalı ve yayınlamalıdır. Yönetmelikte bağımsız üyeler, uzmanlık alanları, komitenin toplantı sıklıkları, komitenin faaliyet alanları ve sorumluluk sınırları özellikle bertilmelidir,
- ✓ Kurumsal Yönetim İlkeleri'nin bir gereği olarak; iç denetim ve Denetim Komitesi raporu işletmelerin internet sitelerinde yayınlamalı ayrıca yıllık faaliyet raporları içinde yer almalıdır,
- ✓ İç denetim biriminin temel görevi Denetim Komitesi ve Yönetim Kurulu'na risk yönetiminin etkinliği hakkında güvence sağlamaktır. Eğer iç denetim birimi bu temel görevin yanısıra ek görevler de üstlenmişse, danışmanlık çerçevesinde risk tanımlamalarda veya risk değerlemelerde görev almak gibi, bağımsızlığını zedeleyecek durumlardan kaçınmalıdır. Bu hassas denge

başarılı bir şekilde sağlandığı takdirde KRY, iç denetim biriminin kurum içindeki etkinliğinin yükselmesine yardımcı olur,

- ✓ İç denetim birimi eğitim faaliyetleri çerçevesinde;
    - İşletme çalışanlarına ve üst yönetime risk terminolojisi ve risklerin anlaşılabilirliği konusunda destek sağlayabilir,
    - Risklerin tanımlaması ve değerlemesi sürecinde gerçekleştirilecek çalıştaylar esnasında destek sağlayabilir.
- ✓ İç denetim müdürü, üst yönetim ve Denetim Komitesi'ni;
    - İşletme faaliyetlerini etkileyebilecek riskler hakkında bilgilendirmeli,
    - Risk yönetimi sisteminin yeterliliği hakkında güvence vermeli,
    - Denetim planına alınmayan riskler hakkında bilgilendirmelidir.
- ✓ İç denetim birimi risk yönetimi sürecinde aşağıdaki alanlarda görev üstlenmemelidir;
    - Kurum amaçlarının belirlenmesi görevi (bir üst yönetim fonksiyonudur),
    - Risk alma istekliliğinin belirlenmesi görevi (bir üst yönetim fonksiyonudur),
    - Riskler hakkında yönetim adına güvence verilmesi görevi (bir üst yönetim fonksiyonudur),
    - Risk tutumu kararının alınması görevi (bir üst yönetim fonksiyonudur),
    - Risk yönetimi sisteminin sorumluluğunun alınması görevi (bir üst yönetim fonksiyonudur),
    - Yönetim adına risklerin yönetilmesi görevi,
    - İç denetim birimi KRY sürecinde yürüttüğü aşamalar için aynı zamanda güvence hizmeti vermemelidir. Bu aşamalar için güvence hizmeti diğer nitelikli taraflardan sağlanabilir.

- ✓ Faaliyet raporlarının güvenilir olmasına olan ihtiyaç; finansal tablo denetiminde olduğu gibi bu raporların da bağımsız denetimden geçirilmesini gerektirmektedir. Bankalar için bu tür bir zorunluluk vardır. Benzer bir düzenleme, İMKB'de hisse senetleri işlem gören firmalar için de yapılmalıdır.
- ✓ Bağımsız denetim raporlarının yanısıra Denetim Komitesi, iç denetim raporlarının, faaliyet raporlarının ve kurumsal yönetim uyum raporlarının tek bir merkezden ilgililere ulaştırılması ve isteyenlerin ulaşımına açık bir şekilde yayınlanması yerinde bir uygulama olacaktır. İç denetim ve risk yönetim sistemi önerilerine ek olarak BDDK düzenlemeleri çerçevesinde bankacılık sistemi için yürütülmekte olan; bağımsız denetim raporlarının BDDK internet sitesinde yayınlanmasına benzer bir uygulama İMKB'de hisse senetleri işlem gören firmalar için yapılmalıdır.

Son olarak SPK'ya göre açıklanması gereken faaliyet raporu ve kurumsal yönetim raporlarının yayınlanma kriterlerine uyulmadığı, hatta hiç yayınlanmadığı ve çeşitli bahanelerle isteyenlere ulaştırılmadığı gerçeğinden hareketle, bu konuda işletmelerin raporların yayınlanması kriterlerine aykırılıklarının giderilmesi sağlanmalıdır.

KAYNAKÇA

KİTAPLAR

Akgül Aziz ve Çevik Osman, **İstatistiksel Analiz Teknikleri,** Emek Ofset, Ankara, 2003.

Anderson Shannon W., Christ Margaret H. and Sedatole Karen L., **Managing Strategic Alliance Risk: Survey Evidence of Control Practices in Collaborative Inter-organizational Settings,** The Institute of Internal Auditors Research Foundation, USA, January 2006.

Armutlu İsmail Hakkı, **İşletmelerde Uygulamalı İstatistik,** Alfa, İstanbul, 2000.

Bozkurt Nejat, **Muhasebe Denetimi,** Alfa, İstanbul, 4. Baskı, 2006.

Chapman Christy and Anderson Urton, **Implementing the Professional Practices Framework,** The Institute of Internal Auditors, USA, 2002.

Chambers Andrew, **Internal Auditing,** London South Bank University, Lecture Notes, London, 2006.

Collier Paul M., Berry Anthony J. and Burke Gary T., **Risk and Management Accounting,** CIMA Publishing, UK, 2007.

El-Dine Dani Saad, **Control Self Assessment Concepts and Applications,** Thomson, Canada, 2005.

Galloway David, **Internal Auditing: A Guide for the New Auditor,** The Institute of Internal Auditors, USA, 1995.

Griffiths David, **Risk Based Internal Auditing: An introduction,** http://www.internalaudit.biz, Version 2.0.3., 15 March 2006.

Griffiths David, **Risk Based Internal Auditing: Three views on implementation,** http://www.internalaudit.biz, Version 1.0.0., 30 January 2006.

Griffiths Phil, **Risk Based Auditing,** Gower Publishing, USA, 2005.

Gupta Parveen P., **Internal Audit Reengineering: Survey, Model and Best Practices,** The Institute of Internal Auditors Research Foundation, USA, 2001.

Güredin Ersin, **Denetim ve Güvence Hizmetleri,** Arıkan, İstanbul, 11. Bası, 2007.

Hillson David and Murray-Webster Ruth, **Understanding and Managing Risk Attitude,** Gower Publishing, USA, 2005.

James M. Patton, John H. Evans and Barry L. Lewis, **A Framework for Evaluating Internal Audit Risk,** The Institute of Internal Auditor Research Foundation, 1982.

Koçel Tamer, **İşletme Yöneticiliği,** Beta, 9. Bası, İstanbul, 2003.

KPMG, **The Financial Statement Audit: Why a New Age Requires an Evolving Methodologies of Large Accounting Firms,** KPMG LLP., USA, 1999.

Lam James, **Enterprise Risk Management From Incentives to Control,** John Wiley & Sons, USA, 2003.

Malhotra Naresh K., **Marketing Research,** USA, Pearson Prentice Hall, 2007.

McNamee David and Selim Georges, **Risk Management: Changing the Internal Auditor's Paradigm,** The Institute of Internal Auditors, USA, 1998.

Merna Tony and Al-Thani Faisal F., **Corporate Risk Management,** John Wiley & Sons, USA, 2005.

Moeller Robert R., **Brink's Modern Internal Auditing,** John Wiley & Sons, 2005.

Moeller Robert, **Sarbanes-Oxley and the New Internal Auditing Rules,** John Wiley & Sons, USA, 2004.

Morris D. Glynis, **An Accountant's Guide to Risk Management,** Tottel Publishing, UK, 2005.

Norman Buckley, **It's a Risky Business: a Practical Guide to Risk Based Auditing,** The Chartered Institute of Public Finance and Accountancy (CIPFA), UK, 2005.

Page Michael and Spira Laura F., **The Turnbull Report, Internal Control and Risk Management: The Developing Role of Internal Audit**, The Institute of Chartered Accountants Scotland, UK, 2004.

Ratliff Richard L., Wallace Wanda A., Sumners Glenn E., McFarland William G. and Loebbecke James K., **Internal Auditing Principles and Techniques,** The Institute of Internal Auditors, USA, 2006.

Rodoplu Gültekin, **Para ve Sermaye Piyasaları,** Isparta, Tuğra Ofset, 2002.

Sawyer Lawrence B., Dittenhofer Mortimer A. and others, **Sawyer's Internal Auditing,** The Institute of Internal Auditors, 2003.

Seyidoğlu Halil, **Bilimsel Araştırma ve Yazma El Kitabı,** Güzem Can Yayınları, İstanbul, 2003.

Sobel Paul J., **Auditor's Risk Management Guide Integrating Auditing and ERM,** CCH Incorporated, USA, 2005.

Spencer Pickett K. H. and Pickett Jennifer M., **Auditing For Managers The Ultimate Risk Management Tool,** John Wiley & Sons, USA, 2005.

Spencer Pickett K. H., **Auditing The Risk Management Process,** John Wiley & Sons, USA, 2005.

Spencer Pickett K. H., **Audit Planning: A Risk Based Approach,** John Wiley & Sons, USA, 2006.

Spencer Pickett K. H., **The Internal Auditing Handbook,** John Wiley & Sons, USA, 2003.

Spencer Pickett K. H., **The Internal Auditor at Work: A Practical Guide to Everyday Challenges,** John Wiley & Sons, USA, 2004.

Vallabhaneni Rao S., **CIA Exam Review Volume 1: Internal Audit Activity's Role in Governance, Risk and Control,** John Wiley & Sons, USA, 2005.

Vallabhaneni Rao S., **Wiley CIA Exam Review Volume 2: Conducting the Internal Audit Engagement,** John Wiley & Sons, USA, 2005.

Wade Keith and Wynne Andy (Editors), **Control Self Assessment For Risk Management and Other Applications,** John Wiley & Sons, USA, 1999. (Chapter 8: Gammon Dave, CSA Workshops as an Integrated Risk-Management Strategy)

Walker Paul L., Shenkir William G. and Barton Thomas L., **Enterprise Risk Management: Pulling it all Together,** The Institute of Internal Auditors Research Foundation, USA, 2002.

MAKALELER

Abela-Reid Carmen, "Risk Based Audit Planning", **The Institute of Internal Auditors-Ottawa Chapter,** 6 January 2005.

Active Academy Ar-Me, "Sürdürülebilir Kurumsal Yönetimin Şartı Etkinlik", **Activeline,** Aralık 2003.

Archambeault Deborah S., "The Relation Between Corporate Governance Strength And Fraudulent Financial Reporting: Evidence From Sec Enforcement Cases", University at Albany –SUNY, **Working Papers,** November 2002.

Argüden Yılmaz, "Kurumsal Yönetim", **Dünya Gazetesi,** 09.08.2002.

Baker C. Richard and Owsen Dwight M., "Increasing The Role of Auditing in Corporate Governance", **Critical Perspectives on Accounting,** Vol. 13, 2002.

Banham Russ, "Enterprising Views of Risk Management", **Journal of Accountancy,** June 2004.

Banham Russ, "Fear Factor: Sarbanes-Oxley offers one more reason to tackle enterprise risk management", **CFO Magazine,** June 2003.

Baraz Barış, "Yönetim Kurullarının Kurumsal Yönetişim Açısından Kritik Önemi: Eskişehir'de Bir Araştırma", **3. Ulusal Bilgi, Yönetim ve Ekonomi Kongresi,** Osmangazi Üniversitesi, Eskişehir, 2004.

Barma Hanif, **"A Good Story Not Told",** Internal Auditing & Business Risk, October 2005.

Beasley Mark S., Clune Richard and Hermanson Dana R., "ERM A Status Report", **Internal Auditor,** February, 2005.

Beasley Mark S., Clune Richard and Hermanson Dana R., Enterprise Risk Management and the Internal Audit Function, **Coles College of Business Kennesaw State University Working Papers,** December 2004.s

Beasley Mark S., Clune Richard and Hermanson Dana R., "Enterprise risk management: An empirical analysis of factors associated with the extent of implementation", **Journal of accounting Public Policy,** Vol: 24, 2005.

Benson Jill, "The Importance of Monitoring", **The Internal Auditor,** August 2007.

Booker Fay M., "An ERM Framework: Developing Effective Risk Management Strategies to Protect Your Organization", **White Paper,** August 2003.

Cain Jackie, "An Approach to Implementing Risk Based Internal Auditing", The Institute of Internal Auditors UK & Ireland, **South-West District Event,** 15 March 2006.

Chambers Richard F., "Assessing Risk in Audit Planning", **European Internal Audit Conference,** 08.10.2004.

Chapman Christy, "The Big Picture – Enterprise Risk Management Services", **Internal Auditor,** June 2001.

Cohen Jeffrey, Krishnamoorthy Ganesh and Wright Arnold M, "Corporate governance and the audit process", **Contemporary Accounting Research,** Vol. 19, No 4, Winter 2002.

Davies Mark, Auditing in the New Millennium, **KPMG's Monograph 2001,** 2001.

De La Rosa Sean, "ERM Based Audit Reports", **Internal Auditor,** December 2005.

Deloitte Touche Tohmatsu, **Managing Business Risks,** 2005, http://www.deloitte.com/growth, 20.02.2005.

Doğu Murat, **"Kurumsal Yönetim Düzenlemeleri",** Sermaye Piyasası Kurulu Meslek Personeli Derneği Dergisi, Sayı 8, Temmuz-Ağustos 2003.

Flesher Dale L., Previts Gary John and Samson William D., "Auditing in the United States: A Historical Perspective", **Abacus,** Vol: 41, No: 1, 2005.

Flexner William A., "Risk Self Assessment: Increasing Speed, Quality and Focus in the Audit Planning Process", **Option Technologies,** Summer 1996.

Fraser Ian and Henry William, "Embedding risk management: structures and approaches", **Managerial Auditing Journal,** Vol: 22, No: 4, 2007

Funston Rick, "Creating a risk-intelligent organization", **Internal Auditor,** April 2003.

Gramling Audrey A. and Myers Patricia M., "Internal Auditing's Role in ERM", **Internal Auditor,** April 2006.

Hespenheide Eric, Pundmann Sandy and Corcoran Michael, "Risk Intelligence: Internal Auditing In A World Of Risk" **Internal Auditing,** Jul/Aug 2007.

Hubbard Larry D., "Assessing Risk", **Internal Auditor,** August 2002.

Knechel Robert W., "The Business Risk Audit: Origins and Obstacles (and Opportunities?)", **3rd EARNet Symposium,** Amsterdam, September 2005.

Kishalı Yunus ve Pehlivanlı Davut, "Risk Odaklı İç Denetim ve İMKB Uygulaması", **Muhasebe ve Finansman Dergisi,** Nisan 2006.

Koutoupis Andreas G. and Tsamis Anastasios, "Reengineering Internal Audit and Compliance Functions within Greek Banks", Fourth European Academic Conference on Internal Audit and Corporate Governance, City University Cass Business School, UK, 6-7 April 2006.

Matyjewicz George and D'arcangelo James R., "Beyond Sarbanes-Oxley", **Internal Auditor,** October 2004.

Matyjewicz George and D'arcangelo James R., "ERM Based Auditing", **Internal Auditor,** November/December 2004.

McCuaig Bruce, "Making The Audit Universe Common Ground", **Internal Auditing,** September-October 2006.

McNamee David and Selim Georges, "Changing Paradigm", **Mc^2 Management Consulting,** http://www.mc2consulting.com/riskart8.htm, (17.11.2006).

Özbek Coşkun, "İç Denetim Uygulamaları", **T.C. Maliye Bakanlığı Twinning Projesi,** İstanbul, 2005.

Özeke Hergüner Bilgen, **Kurumsal Yönetim İlkeleri Uyum Raporu,** www.herguner.av.tr, 23.12.2005.

Özsoy Mehmet Tahir, "Risk Odaklı Denetim, ABD Uygulaması ve Türkiye Uygulaması Açısından Değerlendirilmesi", **Active,** Mart-Nisan, 2004.

Pehlivanlı Davut, "Kurumsal Risk Yönetimi Temelli İç Denetim Araçları", **İç Denetim,** Bahar 2007, Sayı 18.

Protiviti Knowledge Leader, **Risk Assessment Instruction,** www.knowledgeleader.com, 05.06.2007.

Schanfield Arnold and Miller Michael, "A Sustainable Approach to ERM", **Internal Auditor,** April 2005.

Selim Georges and McNamee David, "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change", **International Journal of Auditing,** Vol: 3, 1999.

Spira Laura F. and Page Michael, "Risk Management: The reinvention of internal control and the changing role of internal audit", **Accounting, Auditing & Accountability Journal,** Vol. 16, No:4, 2003.

Goodwin-Stewart, Jenny and Kent, Pamela, "The Use of Internal Audit by Australian Companies", **Managerial Auditing Journal,** 21 (1), 2006.

The Institute of Internal Auditors, "Managing Risk from the Mailroom to the Boardroom", **Tone at the Top,** Issue 18, June 2003.

Walker Paul L., Shenkir William G. and Barton Thomas L., "ERM in Practise", **Internal Auditor,** August 2003.

Uzun Ali Kamil, "Aile İşletmelerinde Kurumsal Yönetim ve İç Denetimin Rolü", **Dünya Gazetesi,** 20.07.2006.

Zacchea Nicholas M., "Risk-based audit target selection can increase the the probability of conducting", **The Journal of Government Financial Management,** Spring 2003.

Yardımcı Ebru, **"Risk ve Kontrollerin Evrimi Hakkında Araştırma Sonuçları",** Uluslararası Kurumsal Yönetim Konferansı, 15 Ocak 2008, İstanbul.

RAPORLAR - STANDARTLAR

Bank For International Settlements, **Internal Audit Charter,** 20.03.2003.

Cadbury Committee, **Report of Committee on the Financial Aspects of Corporate Governance,** UK, 1992.

Canadian Institute of Chartered of Accountants, **Guidance on Control,** Canada, 1995.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Internal Control-Integrated Framework,** AICPA, USA, September 1992.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management-Integrated Framework (Executive Summary),** USA, 2004.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), **COSO Enterprise Risk Management Framework (Draft),** AICPA, USA, 2006.

Country Session: The Republic of Turkey, **Screening Chapter 32: Financial Control**, 30 June 2006, http://www.abgs.gov.tr/index.php?p=190&l=1 (18.07.2007)

Fédération des Experts Comptables Européens, **Risk Management and Internal Control in the EU Discussion Paper,** France, March, 2005.

FTI Consulting Inc., **Internal Audit Charter,** 28.04.2004.

HM Treasury, The Orange Book, Management of Risk-Principles and Concepts, UK, 2004.

Institute of Management Accountants, Statements of Management Accounting, **Enterprise Risk Management: Frameworks, Elements, and Integration,** Institute of Management Accountants, USA, 2006.

Institute of Risk Management (UK), **A Risk Management Standard,** UK, 2002.

International Federation of Accountants, **Internal Control from a Risk Based Perspective,** USA, 2007.

King Committee on Corporate Governance, **King Report on Corporate Governance for South Africa,** Institute of Directors in Southern Africa, 2002.

KPMG, KPMG Metodoloji 2008.

Michael Baker Corporation Charter – Audit Committee, 19.02.2004.

Özeke Hergüner Bilgen, **Kurumsal Yönetim İlkeleri Uyum Raporu,** (www.herguner.av.tr, 23.12.2005)

PricewaterhouseCoopers, **Internal Audit 2012,** PricewaterhouseCoopers, USA, 2007.

PricewaterhouseCoopers, **State of the internal audit profession study: Pressures build for continual focus on risk,** USA, 2007.

Resolver*Ballot, Product Overwiev, http://www.resolver.ca, 17.11.2006.

Sermaye Piyasası Kurulu, **Kurumsal Yönetim İlkeleri,** Şubat 2005.

The Bellsouth Corporation, **Internal Audit Charter,** The Bellsouth Corporation, 2005.

The Financial Reporting Council (Turnbull Committee), **Internal Control: Guidance for Directors on the Combined Code,** UK, 1999.

The Institute of Chartered Accountants England & Wales, **Risk Management and the value added by internal audit**, The Institute of Chartered Accountants England & Wales, UK, 2000.

The Institute of Internal Auditors, **Glossary of Terms,** http://www.theiia.org, 10.09.2006.

The Institute of Internal Auditors Research Foundation (IIARF)-Uluslararası İç Denetim Enstitüsü, **International Standards for the Professional Practice of Internal Auditing,** The Institute of Internal Auditors, USA, 2003, Çeviren Türkiye İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi,** İstanbul, 2003.

The Institute of Internal Auditors Research Foundation (IIARF), **Research Opportunities in Internal Auditing,** The Institute of Internal Auditors, USA, 2003. (Sridhar Ramamoorti, **Chapter 1: Internal Auditing: History, Evaluation, and Prospects,** Kinney William R., **Chapter 5: Auditing Risk Assessment and Risk Management Processes**)

The Institute of Internal Auditors, **Professional Practices Pamphlet: A Perspective on Control-self Assessment,** USA, 1998.

The Institute of Internal Auditors, **Statement of Responsibilities,** The Institute of Internal Auditors, USA, 1990.

The Institute of Internal Auditors-United Kingdom, **Professional Briefing Note: Control and Risk Self Assessment,** The Institute of Internal Auditors - United Kingdom, UK, 1999.

The Institute of Internal Auditors, UK & Ireland, **Position Statement-The Role of Internal Audit in Enterprise-Wide Risk Management,** September 2004.

The Institute of Internal Auditors, UK & Ireland, **Audit Committee Briefing-Gaining Assurance on Risks,** The Institute of Internal Auditors, UK & Ireland, January 2006.

Treadway Commission, **Report of the National Commission on Fraudulent Financial Reporting,** USA, 1987.

TÜSİAD: Risk ve Değer Yönetimi Alt Çalışma Grubu, **Kurumsal Risk Yönetimi,** İstanbul, Aralık 2006.

YASA - YÖNETMELİKLER

TBMM, Bankacılık Kanunu, 01.11.2005 tarih ve 25983 sayılı Resmi Gazete.

Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankaların İç Sistemleri Hakkında Yönetmelik",** 01.11.2006 tarih ve 26333 sayılı Resmi Gazete.

Bankacılık Düzenleme ve Denetleme Kurulu, **"Bankalarca Yıllık Faaliyet Raporlarının Hazırlanmasına ve Yayımlanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik",** 01.11.2006 tarih ve 26333 sayılı Resmi Gazete.

Sermaye Piyasası Kurulu, **"Sermaye Piyasasında Muhasebe Standartları Hakkında Tebliğ",** Seri: XI No: 25, 15.11.2003 tarih ve 25290 sayılı Resmi Gazete.

Sermaye Piyasası Kurulu, **Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ,** Seri: X, No: 22, 12.06.2006 tarih ve 26196 sayılı Resmi Gazete.

TBMM, **Kamu Mali Yönetimi Ve Kontrol Kanunu**, 24.12.2003 tarih ve 25326 sayılı Resmi Gazete.

T.C. Adalet Bakanlığı Türk Ticaret Kanunu Komisyonu, **Yeni Türk Ticaret Kanunu Tasarısı,** 24.02.2005.

USA Congress, **Sarbanes-Oxley Act of 2002,** 30 July 2002.

Maliye Bakanlığı, **"İç Denetçiler Çalışma Usul ve Esasları Hakkında Yönetmelik",** 12.07.2006 tarih ve 26226 sayılı Resmi Gazete.

İNTERNET KAYNAKLARI

http://www.cipfa.org.uk

http://www.coso.org

http://www.darcangelosoftwareservices.com/erm_based_auditing.htm, 19.09.2007.

http://www.deloitte.com/growth

http://www.iia.org.uk

http://www.imanet.org/ima/index.asp

http://www.informationactive.com, 12.03.2007.

http://www.internalaudit.biz

http://www.mc2consulting.com

http://www.knowledgeleader.com

http://www.resolver.ca

http://www.theiia.org

http://www.tkyd.org/tr

www.tide.org.tr

Ek I: "Kurumsal Risk Yönetimi (KRY) Temelli İç Denetim" Anket Formu

	"Kurumsal Risk Yönetimi (KRY) Temelli İç Denetim"	Kocaeli Üniversitesi Bilimsel Araştırma Projeleri Birimi

1. Kişisel Bilgiler ve Görüşler

1.1 Unvanınız:	a) Kaç yıldır şu anki pozisyonunuzda çalışıyorsunuz?				
	< 2 ☐	2-5 ☐	6-10 ☐	11-15 ☐	> 15 ☐

1.2. Riskler karşısındaki eğiliminizi nasıl tanımlayabilirsiniz?	Riskleri reddeden ☐	Risk almayan ☐	Tarafsız ☐	Risk alan ☐	Risklere karşı istekli ☐

1.3. Risk yönetimi faaliyetleri denetim çalışmalarınızda ne kadar yer kaplamaktadır?	Hiç ☐	%0-25 ☐	%26-50 ☐	%51- 75 ☐	%76-100 ☐

1.4. İç denetim birimi hakkında üst yönetimin düşüncesi nedir?	Çok olumsuz ☐	Olumsuz ☐	İlgisiz ☐	İstekli ☐	Çok İstekli ☐

2. Kurum Hakkında Bilgiler

2.1.Kurumunuz bir grup (holding) şirketi midir?	Evet ☐	Hayır ☐

2.2. Kurumunuz grup şirketi ise grup içindeki yerini belirtiniz:	Ana şirket ☐	Bağlı şirket ☐

2.3. Hangi sektörde faaliyet göstermektesiniz?	
a) Finans/Bankacılık	☐
b) Üretim/Perakende	☐
c) Hizmet Sektörü	☐
d) Teknoloji	☐

2.4. Yaklaşık çalışan sayısı?	
a) 250 ve altı	☐
b) 251-500	☐
c) 501-1000	☐
d) 1001-2500	☐
e) 2501 ve üstü	☐

2.5. Kurumunuzun aktif büyüklüğü ne kadardır?	
a) 3 milyon YTL'den az	☐
b) 3 m YTL – 15 m YTL'ye kadar	☐
c) 15 m YTL – 50 m YTL'ye kadar	☐
d) 50 m YTL – 200 m YTL'ye kadar	☐
e) 200 m YTL ve üstü	☐

2.6. Kurumunuzda iç denetim birimi var mı?

Evet ☐
Hayır ☐
(Hayır ise 2.8'den devam ediniz)

2.7. Kurumunuzdaki iç denetçi adedi:

a) 1-3 ☐
b) 4-7 ☐
c) 8-12 ☐
d) 13-18 ☐
e) 18 ve üstü ☐

2.8. Dış kaynaktan denetim destek hizmeti alıyor musunuz?

Evet ☐
Hayır ☐
(Hayır ise 2.10'dan devam ediniz)

2.9. Dış kaynaktan alınan denetim destek hizmetleri nelerdir?

a) Bilgi teknolojileri denetimi ☐
b) Yabancı ülke şubeleri denetimi ☐
c) Geçici özel görevlendirmeler (hile incelemeleri vb) ☐
d) İç denetim bütünleştirme çalışmaları ☐
e) Diğer: ..... ☐

2.10. Kurumunuz iç denetim birimi periyodik olarak kime raporlama yapar ve rapor hazırlama sıklığı nedir?

		Sıklık (Yılda kaç kez)
a) Yönetim Kurulu Başkanı	☐	.....
b) Yönetim Kurulu Üyesi	☐	.....
c) CEO	☐	.....
d) Denetim Komitesi	☐	.....
e) Genel Müdür veya Yardımcıları	☐	.....

2.11. Yıllık iç denetim faaliyetlerinizin odak notası nedir?

	Düşük 1	2	Orta 3	Yüksek 4	5
a) İşletme riskleri temelli denetim	☐	☐	☐	☐	☐
b) Finansal tabloların denetimi	☐	☐	☐	☐	☐
c) Faaliyet denetimi	☐	☐	☐	☐	☐
d) Uygunluk denetimi	☐	☐	☐	☐	☐
e) Bilgi teknolojileri denetimi	☐	☐	☐	☐	☐
f) Kurumsal Risk Yönetimi faaliyetleri	☐	☐	☐	☐	☐
g) Hata araştırmaları	☐	☐	☐	☐	☐
h) Diğer:	☐	☐	☐	☐	☐

2.12. Kurumunuzda Kurumsal Risk Yönetimi (KRY) çalışmaları hangi aşamadadır?

a) Tam olarak faal ☐
b) KRY süreci başladı ama tam olarak faal değil ☐
c) Planlanma aşamasında ☐
d) Henüz düşünülmemekte ☐

2.13. Kurumunuzda risk yönetim faaliyetlerine *yön veren etkenler* hakkındaki düşünceleriniz:	Kesinlikle katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle katılıyorum
a) Yasal etkenler (Mevzuat, yasal düzenleme)	☐	☐	☐	☐	☐
b) Ortakların beklentileri	☐	☐	☐	☐	☐
c) Ticaret hayatının rekabet ortamı	☐	☐	☐	☐	☐
d) Müşteri/tüketici talepleri	☐	☐	☐	☐	☐
e) Yönetim kurulu/üst yönetim talepleri	☐	☐	☐	☐	☐
f) Kurumsal yönetişim ilkeleri	☐	☐	☐	☐	☐
g) Uluslararası standart veya çerçeveler (IIA, COSO)	☐	☐	☐	☐	☐
h) Diğer	☐	☐	☐	☐	☐

2.14. Kurumunuzun risk alma tutumunu nasıl tanımlayabilirsiniz?	Riskleri reddeden	Risk almayan	Tarafsız	Risk alan	Risklere karşı istekli
	☐	☐	☐	☐	☐

2.15. Son iki yıl içinde kurumunuzda risk tanımlama çalışmaları yapıldı mı?	Evet	Hayır
	☐	☐ (Hayır ise 2,18'den devam ediniz)

2.16. Sorunuzun cevabı evet ise risk tanımlama çalışmaları kim tarafından gerçekleştirilmiştir?	
a) Kurum dışı danışmanlar tarafından	☐
b) Risk yönetim birimi tarafından	☐
c) İç denetim birimi tarafından	☐
d) Yöneticilerin katıldığı beyin fırtınası çalışmaları sonucunda	☐
f) Diğer:	☐

2.17. Yanda sıralanan faaliyetlerden kurumunuzda asıl sorumlu kimdir?	Risk tanımlama	Risklerin analizi ve değerlendirmesi	Risk tutumunun belirlenmesi	Raporlama ve izleme	Genel olarak Kurumsal Risk Yönetimi Faaliyetleri
a) CEO / Genel Müdür	☐	☐	☐	☐	☐
b) Yönetim Kurulu	☐	☐	☐	☐	☐
c) Finans Direktörü	☐	☐	☐	☐	☐
d) İç Denetim Müdürü	☐	☐	☐	☐	☐
e) Risk Yöneticisi	☐	☐	☐	☐	☐
f) Hat Yönetimi	☐	☐	☐	☐	☐
g) Diğer					

2.18. Yanda sıralanan faaliyetler kurumunuzda kimler *tarafından yapılmaktadır*?	Risk tanımlama	Risklerin analizi ve değerlendirmesi	Risk tutumunun belirlenmesi	Raporlama ve izleme	Genel olarak Kurumsal Risk Yönetimi Faaliyetleri
a) CEO / Genel Müdür	☐	☐	☐	☐	☐
b) Yönetim Kurulu / Denetim Komitesi	☐	☐	☐	☐	☐
c) Finans Direktörü / Elemanı	☐	☐	☐	☐	☐
d) İç Denetim Müdürü / Elemanı	☐	☐	☐	☐	☐
e) Risk Yöneticisi / Elemanı	☐	☐	☐	☐	☐
f) Hat Yönetimi / Elemanı	☐	☐	☐	☐	☐
g) Diğer					

2.19. Bütün olarak risk yönetimi faaliyetlerinden kim sorumludur?	
a) İç Denetim Müdürü (CAE)	☐
b) Finans Müdürü (CFO)	☐
c) Risk Müdürü (CRO)	☐
d) Diğer	☐

2.20. İç denetim planı hazırlanırken dikkate alınan riskler nelerdir?	
a) Finansal Riskler	☐
b) Operasyonel Riskler	☐
c) Stratejik Riskler	☐
d) İtibar Riski	☐
e) Bilgi Teknolojileri Riski	☐
f) Düzenleme Riski	☐
d) Diğer	☐

2.21. Aşağıda yer alan *metotlar* kurumunuzda ne derece kullanılmaktadır?	i) Risk yönetiminde kullanılmakta: Düşük 1	2	Orta 3	4	Yüksek 5
a) Deneyim, yargı	☐	☐	☐	☐	☐
b) Beyin fırtınası, senaryo anal., SWOT anal.	☐	☐	☐	☐	☐
c) Görüşme, anket	☐	☐	☐	☐	☐
d) Olasılık / etki matrisi	☐	☐	☐	☐	☐
e) İç denetçi veya bağımsız danışman kullan.	☐	☐	☐	☐	☐
f) Stokastik modeller, istatistiki analizler	☐	☐	☐	☐	☐
g) Risk yönetim yazılımı (bilgi işlem desteği)	☐	☐	☐	☐	☐
h) Diğer	☐	☐	☐	☐	☐

2.22. *İşletme temelli riskler* kurumunuz iç denetim faaliyetlerinde hangi aşamalarda dikkate alınmaktadır?	Dikkate alınmamakta	Planlama aşamasında	Raporlama ve izleme aşamasında	Bütün aşamalarda
	☐	☐	☐	☐

2.23. Kurumunuz denetim kültürünü 4 farklı açıdan nasıl tanımlayabilirsiniz?

Denetim Yaklaşımı					Denetçinin Rolü				
Kontrol Odaklı				Risk Odaklı	Bekçi				Danışman
Düşük	Orta		Yüksek		Düşük	Orta		Yüksek	
1	2	3	4	5	1	2	3	4	5
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Denetimin Odak Noktası					Denetçi Nitelikleri				
Geçmiş				Gelecek	Geleneksel Muh-Den				Kur. Risk. Yönetimi
Düşük		Orta		Yüksek	Düşük		Orta		Yüksek
1	2	3	4	5	1	2	3	4	5
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

3. İletişim Bilgileri

Bilimsel araştırma sürecinin bir ürünü olan, yayınlanacak olan makaleyi almak istiyorsanız lütfen isim ve e-mail belirtiniz:	İsim : ..... E-mail : ..... @.....

Ek II: Mülakat Çalışması Soruları

1. Banka ve reel sektörden bir firma ile yapılan mülakatta kullanılan sorular;

A. İç kontrol Ortamına İlişkin Sorular

- Risk yönetimi sürecinde ağırlıklı olarak dikkate alınan çerçeve hangisidir? (COSO, BASEL, COCO gibi)
- Bu çerçevenin tercih edilmesini nasıl açıklayabilirsiniz?
- İç denetimin Kurumsal Risk Yönetimi (KRY) sürecindeki kurumunuzdaki rolü nedir? Uluslararası uygulamaya kıyasla iç denetim biriminin rolü ne olmalıdır? İç denetim birimi sözkonusu fonksiyonları gerçekleştirirken nasıl desteklenmektedir?
- Kurumunuzda iç denetim ve risk yönetimine bakış açısı nasıldır? İki fonksiyon birbirlerinden farklı mı değerlendirilmekte yoksa birbirlerini tamamlayan bütünün bir parçası olarak mı görülmektedir?
- İç denetim biriminiz açısından danışmanlık ve güvence hizmetleri arasındaki hassas dengeyi, özellikle her iki hizmeti verdiğiniz alanlarda risk yönetimi gibi, nasıl sağlıyorsunuz?

B. Risk Tanımlama Sürecine İlişkin Sorular

- Risk tanımlanması sürecinde nasıl bir yöntem kullanıyorsunuz? (Çalıştay, öz değerleme, SOX, ihbar hattı gibi)
- Sizce risklerin tanımlanması sürecinde karşılaşılan en büyük zorluk nedir? (Sürekli değişen riskler gibi)
- Size göre risk ve denetim evreninin oluşturulmasında dikkate alınan risk faktörleri nelerdir?
- Kurumunuzda denetim evreni ortalama kaç adet riski içermektedir nasıl seçilmektedir?
- Denetim evreninin oluşturulması sürecinde üst yönetimin onayı alınıyor mu?
- Makro düzeyde risk ve denetim evreni kim veya kimler tarafından oluşturulmaktadır? Uluslararası standartta ayrıntı olmaması sizi olumsuz

etkiliyor mu? (Mesela denetim evrenine alınmayan bir riskten dolayı yaşanan maddi kayıp sonucu yönetim kurulunun tepkisi gibi.)

- Kurumunuzda risk kayıtlaması (register) kimler tarafından yapılmaktadır ve en üst düzeyde sorumluluk kimdedir?
- Kurumunuzda risk alma istekliliği sınırı (risk iştahı) konusunda kimler yetkilidir? Bu süreçte iç denetçinin katkısı nedir?
- Kurumunuzda risk yönetimi sürecinde bütün riskler dikkate alınmakta mıdır?

2. Bağımsız denetim firması ile yapılan mülakatta kullanılan sorular;

A. İç kontrol Ortamına İlişkin;

- Risk yönetimi sürecinde danışmanlık hizmeti verdiğiniz işletmelerde gözlemlerinize göre ağırlıklı olarak dikkate alınan çerçeve hangisidir? (COSO, BASEL, COCO gibi)
- Bu çerçevenin tercih edilmesini nasıl açıklayabilirsiniz?
- Türkiye'de iç denetimin Kurumsal Risk Yönetimi (KRY) sürecindeki rolü nedir? Uluslararası uygulamaya kıyasla iç denetim biriminin rolü ne olmalıdır? İç denetim bu fonksiyonları gerçekleştirirken nasıl desteklenmelidir?
- Danışmanlık hizmeti verdiğiniz organizasyonlarda iç denetim ve risk yönetimine bakış açısı nasıldır? İki fonksiyon birbirlerinden farklı mı değerlendirilmekte yoksa birbirlerini tamamlayan bütünün bir parçası olarak mı görülmektedir?
- İç denetim biriminin vermiş olduğu danışmanlık ve güvence hizmetleri arasındaki hassas dengeyi, özellikle her iki hizmeti verdiğiniz kurumlarda, nasıl sağlıyorsunuz?

B. Risk Tanımlama Sürecine İlişkin;

- Gözlemlerinize göre risk tanımlanmasında nasıl bir yöntem kullanılmaktadır? (Çalıştay, öz değerleme, SOX, ihbar hattı gibi)

- Gözlemlerinize göre risklerin tanımlanması sürecinde karşılaşılan en büyük zorluk nedir? (Sürekli değişen riskler gibi)
- Gözlemlerinize göre denetim evreninin oluşturulmasında dikkate alınan risk faktörleri nelerdir?
- Gözlemlerinize göre uygulamada denetim evreni ortalama kaç adet riski içermektedir?
- Gözlemlerinize göre denetim evreninin oluşturulması sürecinde üst yönetimin onayı alınıyor mu?
- Danışmanlık hizmeti verdiğiniz kurum/kurumlarda makro düzeyde risk ve denetim evreni kim veya kimler tarafından oluşturulmaktadır? Uluslararası standartta ayrıntı olmaması sizi olumsuz etkiliyor mu? (Mesela denetim evrenine alınmayan bir riskten dolayı yaşanan maddi kayıp sonucu yönetim kurulunun tepkisi gibi.)
- Danışmanlık hizmeti verdiğiniz kurum/kurumlarda risk kayıtlaması (register) kimler tarafından yapılmaktadır ve en üst düzeyde sorumluluk kimdedir?
- Danışmanlık hizmeti verdiğiniz kurum/kurumlarda risk alma istekliliği sınırı konusunda kimler yetkilidir? Bu süreçte iç denetçinin katkısı nedir?
- Danışmanlık hizmeti verdiğiniz kurumlarda risk yönetimi sürecinde bütün riskler dikkate alınmakta mıdır?
- Deneyimlerinize göre risk tanımlama sürecinde iç denetçinin ve denetim komitesinin rolü nedir?

ÖZGEÇMİŞ

Davut PEHLİVANLI, 1979 yılında Kırıkkale'de doğmuş ve ilk, orta ve lise öğrenimini burada tamamlamıştır. 2001 yılında İstanbul Üniversitesi İşletme Fakültesinden mezun olan PEHLİVANLI, 2004 yılında Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü'nde "Türev Ürünler ve UMS 39 Çerçevesinde Muhasebeleştirilmesi" isimli tezi hazırlayarak yüksek lisansını tamamlamıştır. Aralık 2002 tarihinden beri Kocaeli Üniversitesi'nde araştırma görevlisi olarak çalışan PEHLİVANLI, 2006-2007 öğretim yılında doktora tez çalışmalarını yürütmek için gittiği İngiltere'de London South Bank Üniversitesi'nde misafir araştırmacı olarak görev yapmıştır.