# YÖNETİŞİM-RİSK-UYGUNLUK YAKLAŞIMI VE İÇ DENETİM FONKSİYONU İLİŞKİSİ:
# İÇ DENETİM SORUMLULUKLARININ YRU YAKLAŞIMINA ETKİSİ ÜZERİNE YAPISAL EŞİTLİK MODELİ ARAŞTIRMASI

**Doktora Tezi**

**Ahmet ONAY**

**Eskişehir, 2019**

# YÖNETİŞİM-RİSK-UYGUNLUK YAKLAŞIMI VE İÇ DENETİM FONKSİYONU İLİŞKİSİ: İÇ DENETİM SORUMLULUKLARININ YRU YAKLAŞIMINA ETKİSİ ÜZERİNE YAPISAL EŞİTLİK MODELİ ARAŞTIRMASI

**Ahmet ONAY**

**DOKTORA TEZİ**

**Muhasebe Bilim Dalı**
**Danışman: Prof. Dr. Melih ERDOĞAN**

**Eskişehir**
**Anadolu Üniversitesi**
**Sosyal Bilimler Enstitüsü**
**Haziran, 2019**

# JÜRİ VE ENSTİTÜ ONAYI

**Ahmet ONAY'ın "Yönetişim-Risk-Uygunluk Yaklaşımı ve İç Denetim Fonksiyonu İlişkisi: İç Denetim Sorumluluklarının YRU Yaklaşımına Etkisi Üzerine Yapısal Eşitlik Modeli Araştırması"** başlıklı tezi **12 Haziran 2019** tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca **İşletme (Muhasebe)** Anabilim Dalında, **Doktora** tezi olarak değerlendirilerek kabul edilmiştir.

| | |
|---|---|
| **Üye (Tez Danışmanı)** | : Prof.Dr.Melih ERDOĞAN |
| **Üye** | : Prof.Dr.Saime ÖNCE |
| **Üye** | : Prof.Dr.Birol YILDIZ |
| **Üye** | : Prof.Dr.Tunç KÖSE |
| **Üye** | : Doç.Dr.Evrim GENÇ KUMTEPE |

**Prof.Dr.Hasan TUTAR**
**Anadolu Üniversitesi**
**Sosyal Bilimler Enstitüsü Müdürü**

## ÖZET

YÖNETİŞİM-RİSK-UYGUNLUK YAKLAŞIMI VE İÇ DENETİM FONKSİYONU İLİŞKİSİ: İÇ DENETİM SORUMLULUKLARININ YRU YAKLAŞIMINA ETKİSİ ÜZERİNE YAPISAL EŞİTLİK MODELİ ARAŞTIRMASI

Ahmet ONAY
Muhasebe Bilim Dalı
Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Haziran, 2019
Danışman: Prof. Dr. Melih ERDOĞAN

İç denetim, modern dünyada bir meslek olarak kabul görmeye başladığı ilk yıllardan bu yana, faaliyetlerinin kapsamını iş dünyasının ihtiyaçlarına göre belirli aralıklarla güncellemiştir. Yönetişim, risk yönetimi ve uygunluk iç denetim mesleğinin odak noktasında yer alan faaliyetlerdir. İşletmenin başarısını doğrudan etkileyen bu üç kavramın birlikte ele alınması fikri, Yönetişim-Risk-Uygunluk (YRU) kısaltmasıyla ifade edilir. Bu kısaltma, bu üç alanın birbiriyle bağlantılı olarak, bütüncül bir bakış açısıyla ele alınması gerektiğini savunan teknoloji tabanlı bir yaklaşıma evrilmiştir. İşletme yönetimlerinin en büyük destekçisi ve stratejik akıl ortağına dönüşen iç denetim fonksiyonu, yeni yaklaşımların benimsenmesi için güvence ve danışmanlık hizmetlerinin ötesinde, gerektiğinde mesleğin gerektirdiği sınırları aşmadan katılımcı rolünü üstlenmelidir. Çalışmamızda iç denetim ve YRU yaklaşımı teorik olarak ele alınmış ve kavramsal çerçeve değerlendirilmiştir.

Çalışmamızın amacı, iç denetim fonksiyonunun sorumlulukları ile YRU yaklaşımı arasındaki ilişkiyi araştırmaktır. Araştırma kapsamında literatür ve uzman görüşleri doğrultusunda madde havuzu değerlendirme çalışmasıyla elde edilen veri toplama aracına, TİDE üyesi 247 iç denetçiden yanıt alınmıştır. Araştırma modelinin test edilmesi amacıyla iç denetçilerden elde edilen veriler Açımlayıcı Faktör Analizi, Doğrulayıcı Faktör Analizi ve Yapısal Eşitlik Modeli ile analiz edilmiştir. Çalışmanın amaçları doğrultusunda, iç denetimin sorumluluklarına yönelik iç denetçilerin görüşleri, KGK yetki belgesine sahip 96 bağımsız denetçi ve şirketlerinin hisseleri Borsa İstanbul'da işlem gören 72 işletme yöneticisinden oluşturulan örneklem grubunun görüşleriyle karşılaştırılmıştır. Ayrıca görüşler arası farklılıklar, olması gereken durum ve uygulamadaki durum açısından da karşılaştırılmıştır. Örneklem grupları arasındaki

farklılıklar bağımsız örneklemler t testiyle, olması gereken duruma ve uygulamadaki duruma yönelik görüşler arasındaki farklılıklar, eşleştirilmiş örneklemler t testiyle analiz edilmiştir.

Çalışmanın sonucunda, YRU yaklaşımının faydaları ile iç denetimin risk, bilgi teknolojileri, yönetişim sorumlulukları arasında pozitif, üstlenilmemesi gereken risk sorumlulukları ile arasında negatif yönde istatistiksel olarak anlamlı ilişki keşfedilmiştir. İç denetimin sorumluluk sınırlarına uygun davranmasının, YRU yaklaşımının faydalarını artırdığı sonucuna ulaşılmıştır. Ayrıca örneklem gruplarının görüşleri arasında ve olması gereken durum ile uygulamaya yönelik görüşler arasında dikkat çekici sonuçlara ulaşılmıştır.

**Anahtar Sözcükler:** Yönetişim, Kurumsal Risk Yönetimi, Uygunluk, YRU, İç Denetim.

## ABSTRACT

RELATIONSHIP BETWEEN GOVERNANCE-RISK-COMPLIANCE APPROACH AND INTERNAL AUDIT FUNCTION: THE STRUCTURAL EQUATION MODEL RESEARCH ON THE EFFECT OF INTERNAL AUDIT RESPONSIBILITIES ON THE GRC APPROACH

Ahmet ONAY
Department of Accounting
Anadolu University, Graduate School of Social Sciences, June, 2019
Supervisor: Prof. Dr. Melih ERDOĞAN

Since the first years in which internal audit was accepted as a profession in the modern world, it has updated its activities at regular intervals according to the needs of the business world. Governance, risk management and compliance are the focus of the internal audit profession. The idea that these three concepts, which directly affect the success of the enterprise, are dealt with together is expressed by the abbreviation of Governance-Risk-Compliance (GRC). This abbreviation has evolved into a technology-based approach that argues that these three domains should be tackled in a holistic perspective. The internal audit function, which becomes the most important supporter and strategic mentor of the business management, should take on the role of participant beyond the assurance and consultancy services to adopt new approaches. But it should not exceed the limits required by the profession. In our study, the internal audit and the GRC approach were discussed theoretically and the conceptual framework was evaluated.

The aim of our study is to investigate the relationship between the responsibilities of the internal audit function and the GRC approach. Within the scope of the study, the data collection tool obtained by the item pool evaluation study in line with the literature and expert opinions received responses from the TİDE member 247 internal auditors. In order to test the research model, the data obtained from the internal auditors were analyzed with Exploratory Factor Analysis, Confirmatory Factor Analysis and Structural Equation Model. For the purposes of the study, internal auditors' opinions regarding the responsibilities of internal audits were compared with the opinions of the sample group consisting of 72 business executives who are traded in Borsa İstanbul with the shares of companies and 96 independent auditors having KGK authorization certificate. In

addition, the differences between the views were compared in terms of the current situation and the situation in practice. In comparative analysis, independent samples t tests and paired samples t tests were used.

As a result of the study, a statistically significant relationship was found between the benefits of the GRC approach and the risk, information technologies and governance responsibilities of internal audit. A negative correlation was found between the benefits of the GRC approach and the risk responsibilities that should not be assumed. It has been concluded that the compliance of the internal audit with the responsibility limits increases the benefits of the GRC approach. In addition, remarkable conclusions were reached between the views of the sample groups and between the current situation that should be taken and situation in practice.

**Keywords:** Governance, ERM, Compliance, GRC, Internal Audit.

# ÖNSÖZ

Araştırma sürecinin her aşamasında benden desteğini esirgemeyen, hem akademik anlamda hem de hayata dair birçok konuda örnek almaya çalıştığım tez danışmanım Prof. Dr. Melih Erdoğan'a;

Akademik çalışma yapma konusunda bana her zaman yol gösteren, anlayışını ve desteğini hiçbir zaman esirgemeyen değerli hocam Prof. Dr. Saime Önce'ye;

Ders tecrübesi kazanmam konusunda engin bilgisi ve tecrübesinden istifade etmeme fırsat tanıyan, anlayışı ve sabrıyla her zaman yanımda olan değerli hocam Prof. Dr. Nurten Erdoğan'a;

Tezin araştırma modelinin kurgulanmasına ve veri setinin analizine büyük katkı sunan ve desteğini her zaman hissettiren değerli hocam Doç. Dr. Evrim Genç Kumtepe'ye;

Veri toplama sürecine verdiği destek ve arkadaşlığı için değerli hocam Dr. Sezen Uludağ'a;

Dostluğuyla yanımda olan ve çalışmalarım konusunda fikirlerini esirgemeyen Dr. Serdar Benligiray'a;

Araştırma ölçeğinin hazırlanması aşamasında uzman görüşleriyle çalışmama katkı sağlayan hocalarıma;

Ölçeğin anlaşılırlığı konusunda yardım aldığım Anadolu Üniversitesi iç denetçilerine ve iç denetim birimi başkanı Abdullah Efe'ye;

Veri toplama sürecinde desteklerini esirgemeyen TİDE yönetim kuruluna ve onursal başkanı Ali Kamil Uzun'a;

Çalışmalarım sebebiyle kendisini ihmal ettiğim sevgili eşim Begüm'e;

Kendisi üniversite tahsili görmemesine karşın eğitime desteği ve saygısına hayranlık duyduğum üç öğretmen evlat yetiştiren anneannem Cevriye Atay'a;

Hayatımın her anında desteklerini sürekli hissettiren, beni özgür düşünme ortamı içerisinde yetiştiren sevgili annem Nermin Onay ve babam Hamdi Onay'a;

Burada adını sayamadığım üzerimde emeği olan tüm hocalarıma, büyüklerime ve arkadaşlarıma sonsuz teşekkürlerimi sunarım.

12/06/2019

## ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilemeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

Ahmet ONAY

# İÇİNDEKİLER

## TABLOLAR DİZİNİ

**Sayfa**

## ŞEKİLLER DİZİNİ

**Sayfa**

## KISALTMALAR DİZİNİ

**AAA** :American Accounting Association (Amerikan Muhasebeciler Birliği)

**AICPA** :American Institute of Chartered Public Accountant (Amerikan Sertifikalı Muhasebeciler Enstitüsü)

**BDDK** :Bankacılık Düzenleme ve Denetleme Kurumu

**BIS** :Bank for International Settlements (Uluslararası Ödemeler Bankası)

**BT** :Bilgi Teknolojileri

**CAE** :Chief Audit Executive (Denetimden Sorumlu Üst Yönetici- İç Denetim Birimi Yöneticisi)

**CCO** :Chief Compliance Officer (Uygunluktan Sorumlu Üst Yönetici)

**CECO** :Chief Ethics and Compliance Officer (Etik ve Uygunluktan Sorumlu Üst Yönetici)

**CFO** :Chief Financial Officer (Finanstan Sorumlu Üst Yönetici- Mali İşler Müdürü)

**CIA** :Certified Internal Auditor (Sertifikalı İç Denetçi)

**CIO** :Chief Information Officer (Bilişimden Sorumlu Üst Yönetici)

**CISO** : Chief Information Security Officer (Bilişimden Güvenliğinden Sorumlu Üst Yönetici)

**COBIT** :Control Objectives for Information and Related Technology (Bilgi Teknolojileri ve İlgili Teknolojiler için Kontrol Amaçları)

**CoCo** :Criteria of Control (Kontrol Ölçütleri)

**COSO** :Committee of Sponsoring Organizations (Sponsor Organizasyonlar Komitesi)

**CRM** :Müşteri İlişkileri Yönetimi (Customer Relationship Management)

**DFA** :Doğrulayıcı Faktör Analizi

**DRP** :Dağıtım İhtiyaç Planlama (Distribution Resources Planning)

**EDI** :Elektronic Data Interchange (Elektronik Veri Değişimi)

**EDP** :Elektronic Data Processing (Elektronik Veri İşleme)

**FEI** :Financial Executives-International (Finansal Yöneticiler-Uluslararası)

**FRC** :Financial Reporting Council (Finansal Raporlama Konseyi)

**GRC** :Governance-Risk-Compliance (Yönetişim-Risk-Uygunluk)

**IFAC** :The International Federation of Accountants (Uluslararası Muhasebeciler Federasyonu)

**IIA** :The Institution of Internal Auditors (İç Denetçiler Enstitüsü)

**IIARF** :Institute of Internal Auditors Research Foundation (İç Denetçiler Enstitüsü Araştırma Vakfı)

**IMA** :Institute of Management Accountants (Yönetim Muhasebecileri Enstitüsü

**ISA** :International Standards on Auditing (Uluslararası Denetim Standartları)

**ISACA** :Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Birliği)

**ITGI** :Information Technology Governance Institute (Bilgi Teknolojileri Yönetişim Enstitüsü)

**ITIL** :Information Technology Infrastructure Library (Bilgi Teknolojileri Altyapı Kütüphanesi)

**KAP** :Kamuyu Aydınlatma Platformu

**KGİ** :Kapsam Geçerlik İndeksi

**KGK** :Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu

**KGO** :Kapsam Geçerlik Oranı

**MRP** :Malzeme İhtiyaç Planlama (Materials Requirement Planning)

**NIVRA** :Royal Dutch Institute of Chartered Accountants (Hollanda Kamu Muhasebecileri Enstitüsü)

**OCEG** :Open Compliance and Ethics Group (Açık Uygunluk ve Etik Grubu)

**OECD** :Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)

**SAS** :Statement on Auditing Standarts (Denetim Standartları Bildirisi)

**SCM** :Tedarik Zinciri Yönetimi (Supply Chain Management)

**SPK** :Sermaye Piyasası Kurulu

**TİDE** :Türkiye İç Denetim Enstitüsü

**TKYD** :Türkiye Kurumsal Yönetim Derneği

**TMUD** :Türkiye Muhasebe Uzmanları Derneği

**UMUÇ** :Uluslararası Mesleki Uygulama Çerçevesi

**YEM** :Yapısal Eşitlik Modeli

**YRU** :Yönetişim-Risk-Uygunluk

# 1. GİRİŞ

Giriş bölümünde araştırma ile çözümü aranan soruna, araştırmanın amacına, önemine, varsayımlarına ve sınırlıklarına yer verilmiştir.

## 1.1. Sorun

Bilim ve teknolojide son yüzyılda yaşanan gelişmeler, insanlık tarihi boyunca elde edilen gelişmelerin çok ötesindedir. Bilim birikimli bir süreçtir ve ulaşılan seviye daha büyük gelişmelerin habercisidir. Bu bağlamda bilim ve teknolojide ortaya çıkan gelişmeler, giderek daha kısa sürede daha büyük gelişmelerin ortaya çıkmasına sebep olacaktır. Hiç şüphe yok ki, bilimsel ve teknolojik gelişmelerden en fazla etkilenen taraf, insanların sınırsız ihtiyaçlarını gidermek amacıyla hareket eden iş dünyasıdır. İşletmeler üretim süreçleri, lojistik faaliyetleri veya iletişim yöntemleri gibi işletme faaliyetlerini değişen dünyaya uyum sağlayabilmek adına sürekli olarak geliştirmeye çalışmaktadır.

İç denetim fonksiyonu, işletme faaliyetlerinin geliştirilmesini ve iç kontrolün etkin ve verimli hale getirilmesini sağlayan en önemli araçtır. Genel olarak finansal raporlamanın güvenilirliği, yasalara ve düzenlemelere uyum sağlanması ve faaliyetlerin etkin ve verimli şekilde yürütülmesi olarak sıralanan işletme amaçlarına ulaşılmasının güvencesidir. Söz konusu amaçlara ulaşılması adına, yönetim kurulu ve üst yönetime güvence sağlamanın yanında danışmanlık faaliyetleri de yürütür.

1941 yılında IIA (Institute of Internal Auditors - İç Denetçiler Enstitüsü)'nın kurulmasıyla resmiyet kazanan iç denetim mesleği, dünyada yaşanan değişimlere kayıtsız kalmamış ve faaliyetlerinin kapsamını sürekli güncellemiştir. Son yüzyıllık dönemde, iç denetim fonksiyonunun kapsamı; fatura, irsaliye, bordro gibi belgelerin hazırlanması sürecinin günlük kontrolleri veya bağlı ortaklıklar, şubeler ve acentelerin ziyaret edilmesi gibi faaliyetlerden yönetim kuruluna ve üst yönetime danışmanlık yapılması, yeni işletme yaklaşımlarının anlaşılması ve işletmeye tanıtılması, teknolojik araçların kurulumu ve kullanımına kadar uzanmıştır. Meslek, iş dünyasını etkileyen gelişmeler ölçüsünde kendini sürekli güncellemek ve hazır tutmak zorundadır. Özellikle yönetişim, kurumsal risk yönetimi, kurumsal sosyal sorumluluk gibi işletme dünyasını etkileyen yaklaşımlar ve sürekli olarak gelişme gösteren yeni teknolojiler, mesleğin kapsamını genişletmiş, işletmelerde iç denetçilerin yeni roller ve sorumluluklar üstlenmesine yol açmıştır.

IIA; iç denetimin tanımını, standartlarını ve mesleğin kapsamını iş dünyasını etkileyen paradigma değişimlerine, bilimsel ve teknolojik gelişmelere ve işletme

paydaşlarının dönemin ihtiyaçları doğrultusunda iç denetim fonksiyonundan beklentilerine göre yeniden gözden geçirmiştir. 1950'li yıllardan sonra mesleğin kapsamı, yaklaşık olarak 10 yıllık periyodlar halinde yeniden güncellenmiştir. IIA, ihtiyaç gördüğü dönemlerde hazırladığı iç denetimin sorumlulukları raporuyla ve iç denetim tanımında ve mesleki standartlarında yaptığı değişikliklerle, mesleğin kapsamını yeniden belirlemiş ve meslek mensuplarını yönlendirmiştir.

Güncel iç denetim tanımına ve uluslararası nitelik ve performans standartlarına bakıldığında, mesleğin odağında risk yönetimi ve yönetişim faaliyetlerinin geliştirilmesinin yer aldığı anlaşılır. Günümüz işletme çevresinde bilgi teknolojileri ortamında yürütülen risk yönetiminin ve yönetişimin geliştirilmesi amacıyla iç denetçinin bilgi teknolojilerine nasıl yaklaşacağı, BT konusunda ne kadar sorumluluk üstleneceği ve gerekli gördüğünde BT'nin geliştirilmesine ne kadar katkı sunacağı konusundaki yönlendirmeler, mesleki standartlarda ve IIA'nın yayınlarında yoğun şekilde ele alınan konular arasındadır.

Diğer taraftan özellikle küresel muhasebe skandalları sonrası dönemde sayıları giderek artan yasal düzenlemeler, gümrük düzenlemeleri, küresel ticari işbirlikleri ve anlaşmalardan oluşan dış düzenlemeler ve işletmelerin kendi politikalarının uygulanması için gerekli görülen iç düzenlemeler, risk yönetiminde ve etkin yönetişimin geliştirilmesinde işletmelerin karşısına uygunluk problemleri olarak çıkmaktadır. Uygunluk, günümüz işletme çevresinde en önemli risk faktörleri arasında görülmektedir ve iç kontrolün düzenlenmesinde dikkate alınması gereken bir unsurdur. Özellikle son yıllarda uygunluk, iç denetçilerin yoğun mesai harcadığı faaliyetlerin başında gelmektedir.

Son dönemde yönetişim, risk yönetimi ve uygunluğun bir arada düşünülmesini savunan paradigma, YRU (GRC- Governance-Risk-Compliance) kısaltmasıyla ifade edilen yeni bir yönetim yaklaşımı olarak ortaya çıkmıştır. YRU yaklaşımı; strateji, süreçler, teknoloji ve çalışanların düzenlenmesiyle işletmenin etik olarak doğru hareket etmesini ve risk yaklaşımı, iç politikalar ve dış düzenlemeler ile uyumlu olmasını sağlayan, böylece etkinliği ve verimliliği geliştiren işletme çapında yönetişim, risk ve uygunluğu sağlamayı amaçlayan bütüncül bir yaklaşımdır. YRU yaklaşımı, farklı işletme birimlerine faaliyetleriyle ilgili çeşitli faydalar sağlamasının yanında genel olarak, gereksiz faaliyetlerin belirlenmesini sağlayarak maliyetleri azaltır; stratejik ve taktik kararların risk bilgisiyle alınmasını sağlayarak karar süreçlerinde bilginin kalitesini

artırır. Ek olarak YRU yaklaşımının getirdiği bütüncül bakış açısı, ortak paylaşılan güvence evreninden faydalanılması sayesinde iç denetim faaliyetlerinin diğer güvence çalışanlarının faaliyetleriyle bütünleşmesine ve denetimin daha kolay, planlı, anlaşılabilir ve düşük maliyetle yapılmasına katkı sağlar.

İç denetçi, denetimlerinde tüm işletme paydaşlarının haklarını eşit seviyede göz önünde bulundurmalı ve bağımsız olmalıdır. Bağımsızlık meslek mensuplarının sorumluluklarını tarafsızca üstlenmelerini sağlar. İç denetçilere sağladığı faydaların yanında YRU yaklaşımının getirdiği yeni görev ve sorumlulukların sınırının belirlenmesi, mesleğin gerektiği gibi yürütülmesi açısından büyük önem taşır. Mesleki faaliyetlerinde üstlenilmesi gereken bir görevin reddedilmesi veya üstlenilmemesi gereken bir görevin kabul edilmesi, iç denetim faaliyetlerinde başarısız olunmasına ya da iç denetçinin bağımsızlığının zarar görmesine sebep olacaktır.

Teknolojik ve bilimsel gelişmeler, küreselleşen dünyada ortaya çıkan işletme ihtiyaçları ve yeni yönetim yaklaşımları, asıl amacı işletme faaliyetlerinin etkin ve verimli yürütüldüğüne dair güvence sağlamak ve söz konusu faaliyetlerin geliştirilmesi için yönetime danışmanlık yapmak olan iç denetim mesleğinin görev ve sorumluluklarının kapsamını değiştirmiştir. İç denetçilerin IIA'nın rehberlerinde odak noktası haline gelen yönetişim, risk yönetimi ve uygunluk sorumluluklarının sınırlarının farkında olması ve böylece denetimlerin iç denetimin bağımsızlığına zarar vermeyecek şekilde yürütülmesi gerekmektedir. İşletme içinde görev tanımı bilimsel ve teknolojik gelişmeler, işletmenin faaliyette bulunduğu sektör ve işletmenin spesifik ihtiyaçlarına göre değişkenlik gösteren iç denetimin kapsamının ve sorumluluklarının doğru belirlenmemesi, iç denetçinin mesleği yürütmesi için kritik seviyede önemli olan bağımsızlığı ve mesleki başarısı açısından büyük sorunlar yaratır.

Araştırmanın problemi, iç denetimin YRU yaklaşımı kapsamında sorumluluk sınırının belirlenmesidir. İç denetim sürecinde hizmet sunan taraf olan iç denetçilerin, hizmet alan tarafların başında gelen işletme üst yöneticilerinin ve bağımsız denetim sürecinde iç denetçilerle yakın mesai harcayan ve iç denetçilerin geliştirilmesi için çaba harcadığı işletmenin iç kontrolünü değerleyen bağımsız denetçilerin görüşleri, iç denetimin YRU sorumluluklarının belirlenmesi açısından önem taşır. Bu bağlamda "İç denetçilerin, işletme yöneticilerinin ve bağımsız denetçilerin iç denetimin YRU sorumlulukları ile ilgili görüşleri nelerdir?" çalışma kapsamında cevabı aranan ana problem sorusudur.

## 1.2. Amaç

Araştırmanın temel amacı, iç denetimin YRU yaklaşımının işletmede benimsenmesi ve uygulanması için gerekli olan yönetişim, risk yönetimi, uygunluk ve teknolojiye ilişkin sorumluluklarını tespit etmektir. Ayrıca belirlenen iç denetim sorumluluklarının Türkiye'de faaliyet gösteren işletmelerde, iç denetçiler tarafından uygulamada ne denli üstlenildiğini ortaya çıkarmak amaçlanmıştır. Söz konusu sorumlulukların, YRU yaklaşımı üzerindeki etkisinin belirlenmesi çalışmanın bir diğer amacıdır.

İç denetimin YRU sorumluluklarının belirlenmesi amacıyla iç denetçilerin yanı sıra iç denetçilerin güvence ve danışmanlık faaliyetlerinin tarafı olan üst yöneticiler ile bağımsız denetim sürecinde denetimin kapsamını ve denetim riskini belirlemek amacıyla işletmenin iç kontrolünü değerlendiren ve gerekli gördüğü alanlarda iç denetçilerle işbirliği yapan bağımsız denetçilerin görüşlerine başvurulmuştur. İç denetim mesleğinin YRU yaklaşımına ilişkin sınırlarının belirlenmesi, iç denetçilerin YRU yaklaşımı ile ilgili farkındalığının artırılmasını sağlayacaktır. Ayrıca işletme yöneticilerinin ve bağımsız denetçilerin söz konusu sorumluluklara ilişkin beklenti ve görüşleri elde edilerek, iç denetim faaliyetlerine yön verilmesinin sağlanması çalışmanın amaçlarındandır.

Çalışmada veri toplama yöntemi olarak anket tercih edilmiştir. Elde edilen veriler nicel yöntemlerle ayrıntılı olarak analiz edilmiştir. Çalışmaya yön veren araştırma soruları şunlardır:

1. İç denetçilerin, iç denetimin YRU yaklaşımı kapsamındaki sorumluluklarına ilişkin görüşleri nelerdir?
2. Bağımsız denetçilerin ve işletme yöneticilerinin, iç denetimin YRU yaklaşımı kapsamındaki sorumluluklarına ilişkin görüşleri nelerdir?
3. İç denetçilerin, YRU yaklaşımı kapsamında iç denetimin sorumluluklarını uygulamada ne kadar üstlendiklerine ilişkin görüşleri nelerdir?
4. Bağımsız denetçilerin ve işletme yöneticilerinin, YRU yaklaşımı kapsamında iç denetimin sorumluluklarını uygulamada ne kadar üstlendiklerine ilişkin görüşleri nelerdir?
5. İç denetçilerin YRU yaklaşımının faydalarına ilişkin görüşleri nelerdir?
6. Bağımsız denetçilerin ve işletme yöneticilerinin, YRU yaklaşımının faydalarına ilişkin görüşleri nelerdir?

### 1.3. Önem

IIA kurulduğu 1941 yılından bu yana, iç denetimin tanımını ve standartlarını işletme dünyasında yaşanan değişime ve gelişmelere paralel olarak güncellemektedir. İşletme çevresinde yaşanan değişim sonucunda ortaya çıkan ihtiyaçlara cevap verebilmek adına iç denetim mesleğinin kapsamı ve iç denetçilerin sorumlulukları değişmektedir. İç denetim mesleğinin YRU konusundaki sorumluluklarını ortaya çıkarmak ve bu sorumlulukların uygulamada ne kadar üstlenildiğini tespit etmek, mesleğin geliştirilmesi amacıyla yapılan yerel ve uluslararası düzenlemelere katkı sağlanması açısından büyük önem taşır. Araştırma sonucunda elde edilen veriler, iç denetim mesleğinin sorumluluklarının belirlenmesinin ötesinde, ortaya çıkan yeni ihtiyaçlar sonucunda, iç denetimin tanımı ve standartlarının revize edilmesine katkı sağlayacaktır.

İç denetçilerin yeni yaklaşımlar ve teknolojilerin geliştirilmesi sonucunda üstlenmeleri gerekebilecek yeni sorumlulukları hakkında araştırma sonucunda elde edilen bakış açısı, iç denetçilere mesleki faaliyetlerini geliştirme imkânı sunacaktır. Ayrıca araştırma, iş dünyasının iç denetim fonksiyonundan mesleğin objektifliğini ve bağımsızlığını zedelemeden nasıl ve ne ölçüde yararlanması gerektiğinin sınırlarını çizer. Araştırma, iç denetimin mesleki objektifliğine ve bağımsızlığına zarar verecek faaliyetlerin iç denetçinin görev tanımına dâhil edilmemesinin sağlanmasında yol gösterici olması açısından önemlidir.

YRU yaklaşımının benimsenmesi, işletme faaliyetlerinin ve iç kontrolün geliştirilmesini sağlamasının yanında spesifik olarak iç denetim mesleğine faydalar sağlar. İç denetim sorumluluklarının işletmenin iç kontrolünü geliştiren, işletme faaliyetlerine değer katan ve özellikle risk yönetimi, iç denetim ve uygunluk gibi güvence faaliyetlerinin etkinliğini arttıran YRU yaklaşımı üzerindeki etkisini ortaya çıkarmak, iç denetimin etkinliğini ve kalitesini artıran bir yaklaşım olan YRU konusundaki farkındalığın artırılması yönüyle önemlidir.

Çalışmada iç denetim, çalışmanın kapsamına uygun olarak tarihsel gelişimi ve ortaya çıkış sebepleriyle ve YRU'nun büyük ölçüde işletmenin iç kontrolünü etkileyen bir yaklaşım olması sebebiyle iç kontrol çerçeveleriyle birlikte ele alınmıştır. Çalışmada YRU yaklaşımı, üç hatlı savunma modelinde ele alındığı şekliyle iç denetime ve diğer güvence fonksiyonlarına faydalarını vurgulayacak şekilde incelenmiştir. Tarihsel süreçte YRU yaklaşımından bağımsız olarak gelişme gösteren YRU bileşenleri ise, iç denetim ile ilişkilendirilerek ele alınmıştır. Literatür taraması sonucunda iç denetimin

sorumluluklarına odaklanan çok sayıda çalışmanın olduğu ancak YRU yaklaşımı-iç denetim ilişkisini inceleyen çalışmaların sayısının çok az olduğu anlaşılmıştır. Çalışmamız iç denetimin YRU sorumluluklarını nicel analizler ile incelemesi yönüyle literatürde bulunan çalışmalardan ayrılır.

### 1.4. Varsayımlar

Araştırmanın veri toplama aracı olan ankete katılan iç denetçi, işletme yöneticisi ve bağımsız denetçilerden oluşan araştırma örnekleminin, ölçek maddelerine ilişkin görüşlerini samimi ve doğru şekilde ifade ettikleri varsayımıyla hareket edilmiştir. Ayrıca katılımcıların, ankete katılım öncesinde kendilerine verilen bireysel bir değerlendirme yapılmayacağı ve kişisel verilerinin anonim hale getirileceği güvencesine istinaden; mesleki unvanlarını, iç denetçilerle olan ilişkilerini ve çalıştıkları şirketin imajını bir kenara bırakarak nesnel şekilde görüşlerini yansıttıkları varsayılmıştır.

Ölçek maddelerinin açıklığı, sadeliği ve anlaşılırlığı üzerinde, uzman görüşlerine başvurularak yapılan veri derleme aracının elde edilmesi aşamasında uzun zaman ve emek harcanarak titizlikle durulmuştur. Ayrıca yalnızca aktif olarak mesleğin içinde olan denetim yetki belgesine sahip bağımsız denetçilerin ve Borsa İstanbul'da işlem gören şirketlerin yöneticilerinin ankete katılması istenmiştir. Araştırmanın hedef kitlesinin bilgi seviyesi yüksek katılımcılardan oluşması, soruların anlaşılmasını kolaylaştıran bir etkendir. Ölçek maddelerinin anlaşılırlığını sağlamaya yönelik söz konusu çabalara karşın, soruların katılımcılar tarafından aynı şekilde anlaşıldığı araştırmanın başka bir varsayımıdır.

### 1.5. Sınırlıklar

Araştırma, veri toplama aracı olarak kullanılan ankete gönüllü olarak katılım gösteren katılımcılardan elde edilen veriler ile sınırlıdır.

Araştırmada kullanılan anket; ölçek maddeleri üzerinde tek tek durularak, uzman görüşlerinden istifade edilerek ve araştırmanın hedef kitlesinde bulunan kişilerle tartışılarak, özenli bir süreç sonucunda elde edilmiştir. Araştırma, ölçek maddeleriyle elde edilen verilerle sınırlıdır.

Araştırma probleminin arka planındaki kuramsal bilginin tam olarak açıklanabilmesi için literatürün yeterli sayı ve nitelikte olması gereklidir. Araştırmamızda

iç denetçilerin YRU sorumluluklarını bir arada ele alan nicel bir saha çalışmasının olmaması karşılaşılan zorluklardandır.

Araştırmanın örneklemi, ekonomik kısıtlar yüzünden sadece Türkiye'de yerleşik katılımcılar ile sınırlı tutulmuştur.

## 2. İÇ DENETİM

Sanayi Devrimi sonrasında gelişen ekonomik ortam, büyük ölçekli işletmelerin sayısının giderek artmasına yol açmıştır. İşletme büyüklüklerinin artması, modern işletme yönetimini derinden etkilemiştir. Günümüzde karmaşıklaşan iş dünyası, risk faktörlerindeki artış ve teknolojide yaşanan gelişmeler, işletme yöneticilerinin işlerini daha da zorlaştırmaktadır. İşletme yönetiminin birtakım yetki ve sorumluluklarını çalışanlarına devretmeleri bir zorunluluk haline gelmiştir. İşletme çalışanlarının sorumluluklarını başarıyla yerine getirmeleri, işletmelerin amaçlarına ulaşmaları açısından büyük önem taşır. İşletme yönetimine çalışanlarının üstlendikleri görev ve sorumlulukların etkin bir şekilde yerine getirildiğine dair güvence sağlayan ve gerektiğinde işletme faaliyetlerini geliştirmek amacıyla danışmanlık eden fonksiyon iç denetimdir.

Teknolojik gelişmelerin hız kazanması, işletme faaliyetlerinin küreselleşme ve artan rekabetin etkisiyle karmaşık bir hal alması ve çağdaş işletme yönetimindeki gelişmeler, iç denetimin gerekliliğini perçinlemiş ve sunduğu hizmetlerin kapsamını modern anlamda ortaya çıktığı tarih olan 1941 yılından bu yana giderek genişletmiştir. Günümüzde işletme yönetiminden sorumlu kişilerin en büyük yardımcısı, işletmenin kendi çalışanları olan ancak mental anlamda objektif ve bağımsız olarak hareket eden iç denetçileridir. Bir işletmede iç denetim hizmetinin varlığı, işletmenin doğru yolda olduğunun makul ölçüler içerisinde güvencesidir.

Çalışmamızın bu bölümünde, iç denetim genel anlamda denetim kavramı ve denetim talebine ilişkin teoriler ile ilişkilendirilerek ve tarihsel gelişimi çerçevesinde açıklanmıştır. Ayrıca iç denetimin işletmede etkin bir iç kontrol sisteminin geliştirilmesi amacına istinaden, iç kontrol ile ilişkisi ve iç kontrol çerçeveleri ele alınmıştır.

### 2.1. Denetim Kavramı

Denetim teorisinin önemli bir köşe taşı olan Mautz ve Sharaf'ın 1961 yılında yayımladıkları Denetim Felsefesi isimli eserden günümüze kadar, denetimin en geniş kapsamlı ve üzerinde uzlaşılmış tanımı, Amerikan Muhasebeciler Birliği (American Accounting Association (AAA) Temel Denetim Kavramları Kurulu (Committe on Basic Auditing Concepts) raporunda yer almaktadır (Erdoğan, 2005, s.1). Bu tanıma göre;

"*Denetim, ekonomik faaliyetler ve olaylara ilişkin savlarla, kabul edilmiş ölçütler arasındaki uygunluğun derecesini araştırmak ve sonuçlarını ilgili kullanıcılara iletmek amacıyla nesnel biçimde kanıt toplayan ve değerleyen sistematik bir süreçtir*."

Bu tanım aslında çok yönlü, ayrıntılı ve geniş bir sürecin özlü bir ifadesidir. Yılların içinden gelen deneyimlere ve çalışmalara dayalı olarak yapılmıştır ve birçok şeyi açıklamaktadır. Tanım, unsurları ele alınarak daha iyi anlaşılabilir (Erdoğan, 2005, s.1):

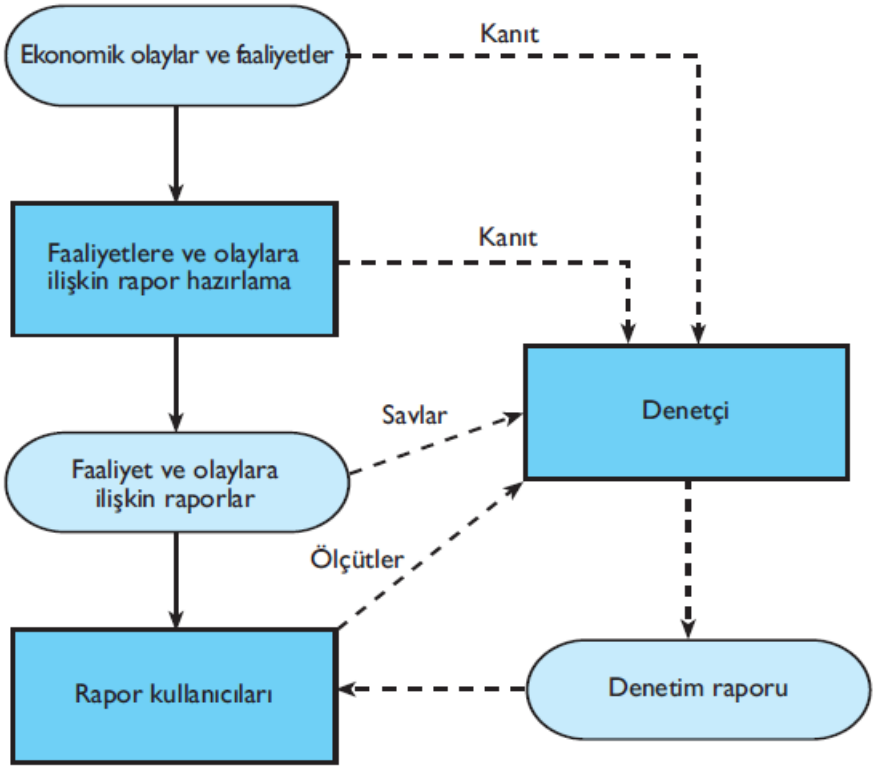
Denetçi tarafından toplanan ve değerlendirilen kanıtlar, ekonomik faaliyetler ve olaylar hakkındaki savlarla ilgilidir. Kanıt toplama amaçlarının temelinde, yönetimin savlarının kanıtlarla ispatlanması yer alır. Savlar yönetim tarafından finansal tablolarda sunulmuştur. Yönetimin ekonomik faaliyetler hakkındaki savlarından biri, işletmenin sahip olduğu varlıkların tamamının bilanço tarihi itibariyle gerçekte var olduğu şekliyle bilançoda raporlandığıdır. Varlıkların hayali değil, gerçek olmasına var olma savı denir. Dahası, yönetim tüm bu varlıkların sahibinin işletme olduğunu iddia eder. Varlıkların başka bir kimseye ait olmaması, haklar ve yükümlülükler savını ifade eder. Denetçi savlarla önceden belirlenmiş ölçütler arasındaki uygunluğun derecesini belirlemelidir. Denetim programı doğrulama, sorgulama, gözlem ve fiziksel inceleme yoluyla birçok savı test eder. Denetçi, finansal tablolarda sunulan ve açıklanan savların, hesaplarda Uluslararası Finansal Raporlama Standartları, yerel standartlar veya yasal düzenlemeler gibi bir finansal raporlama çerçevesine uygun şekilde yer alıp almadığını belirlemek için kanıtları inceler (Hayes vd., 2005, s.11).

Denetçi yönetimin savları hakkında topladığı kanıtlarla kabul edilmiş ölçütleri karşılaştırarak, bunlar arasında uygunluğun derecesini belirleme çabası içine girecektir. Söz konusu ölçütler yasalardan kaynaklanabileceği gibi, yönetimin koyduğu kurallar ve politikalardan da oluşabilir. Ancak en önemli ölçütler seti, finansal tabloların hazırlanmasında yol gösterici olan Genel Kabul Görmüş Muhasebe İlkeleridir (Erdoğan, 2005, s.2).

Denetim sürecinin son aşaması, denetçinin bulgularını rapor kullanıcılarına iletmesini sağlayan denetim raporunun hazırlanmasıdır. Birbirinden farklı biçimde raporlar hazırlanabilir ama hepsi okuyucularına önceden belirlenmiş ölçütlerle denetim bilgisi arasındaki uygunluğun derecesi hakkında bilgi verir. Finansal tablo denetimlerinde genellikle teknik özelliklere sahip raporlar hazırlanırken, küçük bir birimin etkinliğinin faaliyet denetiminde basit sözlü bir rapor sunulabilir (Arens vd., 2012, s.5). Denetim raporunun potansiyel ilgili kullanıcıları; ortaklar, kredi kurumları, işletme yönetimi,

çalışanlar, tedarikçiler, araştırmacılar, devlet kurumları ve yatırımcılar gibi farklı taraflardan oluşur.

Sistematik süreç, denetimin yürütülmesi için kapsamlı ve iyi planlanmış bir yaklaşımın geliştirilmesi gerektiğini ifade eder. Bu yaklaşım, kanıtların nesnel bir biçimde toplanması ve değerlendirilmesini gerektirir. Başka bir ifadeyle, denetçi kanıtın ilgili ve geçerli olup olmadığını objektif bir şekilde araştırmalı ve değerlendirmelidir. Denetimler arasında kanıtın şekli, niceliği ve güvenilirliği değişkenlik gösterebilir, fakat her denetimde kanıt elde etme ve değerlendirme süreci, denetçinin faaliyetlerinin büyük çoğunluğunu bir araya getirir (Messier vd., 2016, s.12). Denetim süreci, Şekil 2.1'de özlü bir şekilde gösterilmiştir.




**Şekil 2.1.** *Denetim Süreci (Erdoğan, 2012, s. 4)*

Şekilde yer aldığı gibi denetçi, ekonomik olaylar ve faaliyetler ve bunlara ilişkin rapor hazırlama sürecinden kanıtlar toplayarak, faaliyet ve olaylara ilişkin raporlarda yönetim tarafından ileri sürülen savları, kabul edilmiş ölçütlerle karşılaştırmaktadır. Daha sonra söz konusu savlarla ölçütler arasındaki uygunluğun derecesini hazırladığı denetim raporuyla ilgili kullanıcılara iletmektedir (Erdoğan, 2005, s.3).

## 2.2. Denetimin Tarihsel Gelişimi

Denetim, Hristiyanlıktan çok önce tarih sahnesinde yer almıştır. Antropologlar İsa'dan yaklaşık olarak 3000 yıl önceye, Babil zamanına uzanan denetim faaliyeti kayıtlarına ulaşmışlardır. Ayrıca antik Çin, Yunan ve Roma'da da denetim faaliyeti yer almaktaydı. Denetçi 'auditor' kelimesinin Latince anlamı işiten veya dinleyen anlamına gelir çünkü Roma'da denetçiler, vergi görevleri ve işlerinin sonuçları konusunda kamuoyu açıklamalarında bulunan -çiftçiler gibi- vergi mükelleflerini dinlerlerdi (Hayes vd., 2005, s.2).

Eski Mısırda firavunlar denetçilerine karşı müsamahasızlardı. Her bir kraliyet deposunda iki denetçi kullanılırdı. Bunlardan biri malları deponun kapısına geldiklerinde sayar, ikincisi ise mallar depolandıktan sonra sayardı. Daha sonra iki denetçinin kayıtları karşılaştırılırdı. Eğer kayıtlar arasında bir farklılık bulunursa, denetçilerin ikisi de öldürülürdü (Hayes vd., 2005, s.2).

Roma İmparatorluğu'nun çöküşünden sonra denetim, İtalyan şehir devletlerinde gelişme göstermiştir. Floransa, Ceneviz ve Venedikli tacirler Eski Dünya'nın zenginliklerini Avrupa Anakarasına taşıyan ticaret gemisi kaptanlarının hesaplarını doğrulamak için denetçilerden faydalanmışlardır. Bu dönem boyunca denetimin önceliği hileleri önlemektir (Brown, 1962, s.697).

İtalya'da büyük tüccar birliklerinin kurulmasıyla, Orta Çağ'ın sonunda kar maksimizasyonu davranışı gelişme göstermiştir. Ticaret artık bireysel ticaret seyyahlarının alanından çıkmış; Venedik, Floransa ya da Pisa'daki büyük tüccar birliklerinin şaşalı masalarında merkezden yönetilmeye başlamıştır. Bunun sonucunda, iletişim önemli hale gelmiştir. Bundan dolayı, çift taraflı kayıt sisteminin ilk defa 20 Kasım 1494'te İtalya'da Luca Pacioli'nin Summa de Aritmetica adlı eseriyle ortaya çıkmış olması hiç de şaşırtıcı değildir (Hayes vd., 2005, s.2). Muhasebe biliminin doğuşunda rol oynayan temel motivasyon, denetim ihtiyacı olmuştur.

Sanayi Devrimine kadar denetim, resmen kabul edilmiş bir meslek değildi. Buna karşın antik dönemden beri denetim faaliyeti değişik biçimlerde de olsa yürütülmüştür. Denetimin ilk defa tarih sahnesine çıktığı dönemden Sanayi Devrimine kadarki süreçte, denetim faaliyeti yürütülürken her işlem eksiksiz bir şekilde tek tek denetlenmekteydi. Bu açıdan %100'lük bir inceleme ve doğrulama söz konusuydu. Denetimin amacı, hilelerin önlenmesi ve işletmeye hizmet sunanların dürüstlük derecesinin saptanmasıydı.

1900'lü yıllara kadar olan dönemde, denetimin amacı ve yönteminde önemli bir değişiklik yaşanmamıştır (Güredin, 2000, s.7).

Sanayi Devriminin bütün dünyaya yayıldığı ülke olan İngiltere'de 19. yüzyılda denetim mesleği büyük önem kazanmıştır. 1900 yılında İngiltere'de çıkarılan bir yasa ile sınırlı sorumlu şirketlere denetim zorunluluğu getirilmiştir. Günümüzde de varlığını sürdüren dört büyük denetim firmasından biri olan Deloitte, 1845 yılında Londra'da William Deloitte tarafından kurulmuştur (Yıldırım vd., 1995, s.149).

Modern denetim faaliyetleri, Sanayi Devriminin sonucunda modern anlamda işletmelerin kurulmasına kadar uzanır. 1853 yılında Muhasebeciler Derneği (The Society of Accountants) Edinburgh'da kurulmuştur. Büyük Britanya'da kurulan birçok kuruluş, 1880 yılında İngiltere ve Galler'de Sertifikalı Muhasebeciler Enstitüsü adıyla bir araya gelmiştir. Bu ülke çapındaki enstitü, örneğin 1886'da Amerika'da ya da 1895'de Hollanda'da kurulan enstitü gibi 19. yüzyılın sonunda Batı Dünyası'nda kurulan bütün enstitülerin öncülüdür (Hayes vd., 2005, s.2).

Modern kamu muhasebeciliği alanındaki ilk kurum Birleşik Krallık'ta kurulmuş ve daha sonra bu alandaki kurumlar tüm dünyaya yayılmıştır. Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü'nün (AICPA) 1887 yılında kurulmasıyla, profesyonel denetim mesleğinin ağırlık merkezi Amerika'ya kaymış ve o zamandan beri de öyle kalmıştır. Muhasebede 20. yüzyılda yaşanan gelişmelerin birçoğu Amerika kaynaklıdır. 20. yüzyılda profesyonel muhasebe ve denetim birlikleri, üyeleri için sertifikasyon programları geliştirmiştir. Ayrıca mesleğin metodolojileri, teknik temelleri ve etik kurallarının sistemleştirilmesi ve tanımlanması için denetim standartları geliştirilmiştir (O'Regan, 2003, s.2).

20. yüzyılın ilk yarısında meydana gelen önemli bir değişiklik, işletmelerin finansal durumlarıyla ilgilenen çıkar gruplarının oluşmasıdır. Bu durum denetimin amacını, finansal tabloların doğruluğu hakkında onay verme şekline dönüştürmüştür. Amaçlardaki değişim, tekniklerde de değişime yol açmış ve örnekleme teknikleri daha fazla kullanılmaya başlanmıştır. 20. yüzyılın ikinci yarısındaysa, denetçiler işletmelerde etkin bir iç kontrolün gerekliliğine kanaat getirmişler ve denetim faaliyetlerinde iç kontrolü incelemeye başlamışlardır.

Günümüzde 4. Endüstri Devriminin (Teknoloji Devrimi) gerçekleşmesiyle birçok meslek gibi denetim mesleğinin de kapsamı ve kullandığı teknikler gelişme göstermiştir. Artık denetçi, finansal tablolar ile beraber uzman sistemler, yapay zekâ ve yapay sinir

ağlarından oluşan karar destek sistemleri hakkında da görüş oluşturmak zorundadır. Denetim teknikleri büyük ölçüde bilgi teknolojileri ortamında yürütülmekte ve teknolojiden yoğun şekilde faydalanılmaktadır. Ayrıca günümüzde ilgili kullanıcıların bilgiye üretildiği anda ya da en azından mümkün olan en kısa zamanda erişmek istemeleri sonucunda denetim anlayışı değişmiş, bilgiye ortaya çıktığı anda ya da çok kısa bir süre sonra denetçi tarafından güvence verilmesini amaçlayan sürekli denetim yaklaşımı ortaya çıkmıştır.

Dünyadaki ekonomik gelişmeler çerçevesinde denetimde meydana gelen değişim Tablo 2.1'de evreler halinde gösterilmiştir:

**Tablo 2.1.** *Denetimin Tarihsel Gelişimi (Güredin, 2000, s. 7; Kavut, Taş, Şavlı, 2009, s. 45)*

| Dönem | Denetim Yaklaşımı | Denetimin Amacı | İlgili Taraflar (Bilgiyi Kullananlar) |
|---|---|---|---|
| **Sanayi Devrimi Öncesi** | Belge ve kayıtların %100'ünün incelenmesi | Hata ve hilelerin bulunması | İşletme sahipleri |
| **Sanayi Devriminden 1900'lü Yıllara Kadar** | Belge ve kayıtların %100'ünün incelenmesi | Hata ve hilelerin bulunması | Ortaklar ve işletmeye borç verenler |
| **1900-1950** | Belge ve kayıtların %100'ünün incelenmesi ve örneklemeye başvurma | Bilanço ve gelir tablosunun doğruluğunu onaylama | Ortaklar, işletmeye borç verenler, devlet |
| **1950-1990** | Örnekleme yoluyla denetim, istatistiki örneklemenin yaygınlaşması | Finansal tabloların doğruluğu hakkında görüş oluşturma | Ortaklar, kredi kuruluşları, devlet, sendikalar, çalışanlar, tüketiciler, tedarikçiler ve diğer ilgili kesimler |
| **1990-2010** | Örnekleme yoluyla denetim, risk odaklı denetim ve bilgi teknolojileri ortamında denetim | Finansal tabloların doğruluğu hakkında görüş oluşturma | Ortaklar, kredi kuruluşları, devlet, sendikalar, çalışanlar, tüketiciler, tedarikçiler ve diğer ilgili kesimler |
| **2010 ve sonrası** | 4. Endüstri Devrimiyle birlikte denetimde tamamen bilgi teknolojilerinden faydalanma ve bilgiye ortaya çıktığı anda ya da çok kısa bir süre sonra denetçi tarafından güvence verilmesini sağlayan sürekli denetim yaklaşımının gelişmesi, örnekleme yapmak yerine büyük veri analitiğiyle verinin %100'ünün incelenmesi | Finansal tablolarla beraber uzman sistemler, yapay sinir ağları ve yapay zekâ gibi karar destek sistemleri hakkında görüş oluşturma | Sermaye piyasalarının derinleşmesi ve teknolojinin sunduğu imkânlar ve küreselleşmeyle ortadan kalkan sınırlar, Dünya'daki her bir bireyi ve kurumu potansiyel ilgili taraf haline getirmiştir. |

## 2.3. Denetim Talebine İlişkin Teoriler

Denetimle ilgili konuların büyük çoğunluğu teorik olarak değil, tamamen uygulamaya yönelik olarak ele alınır. Denetim bir pratikler, yordamlar, yöntemler ve teknikler serisidir. Uygulamada daha az ihtiyaç duyulan açıklamalar, tanımlar, savlar ve görüşler ise, genellikle teori olarak ifade edilir. Denetim teorisi, birçok temel varsayım ve kavramdan oluşur. Denetim teorisinin anlaşılması, denetim sanatının uygulanması ve gelişmesine doğrudan katkı sağlayacaktır. Denetim teorisi, denetçilerin karşılaştığı birçok karmaşık problemin rasyonel çözümü için hem uygulayıcıları hem akademisyenleri yönlendirebilir (Mautz & Sharaf, 1961, s.1).

Denetim talebine ilişkin teoriler, denetimin genel bir çerçevesini sağlar ya da en azından denetimin anlaşılmasına yardımcı olur. Mautz ve Sharaf teorinin amacını şöyle ifade etmiştir (Mautz & Sharaf, 1961, s.4-5):

"Denetim teorisiyle ilgili ciddi ve ayrıntılı bir araştırma yapmanın nedenlerinden biri, şimdi cevabını bulmakta zorlandığımız problemlerin çözümlerini ya da en azından çözümleriyle ilişkili ipuçlarını sağlayacağına olan beklentidir."

Denetim teorisi, ilk etapta, denetime neden ihtiyaç duyulduğunun açıklanmasına destek olur. İşletme ve çevresi arasında iletişime sahip olan denetim sürecinin rolü ve amacı nedir? Ayrıca denetim teorisi, denetim için çok önemli olan varsayımları ve anahtar kavramları açıklamak için uğraşır. Denetim süreci ve denetim faaliyetlerini yönlendiren yasaları da açıklar. Bir işletmede farklı kesimler arasında karşılıklı ilişkilerin anlaşılmasını sağlar (Ittonen, 2010, s.2).

### 2.3.1. Polis memuru teorisi (Policeman theory)

Denetim hizmetine olan talebi açıklamaya çalışan polis memuru teorisine göre, denetim işi matematiksel doğruluğa ve hilelerin bulunması ve önlenmesine odaklanmalıdır (Chukwunedu & Okoye, 2011, s.6). Denetçinin görevi, bir polis gibi hilelerin bulunması mıdır? Bu teoriye göre, denetçinin eylemleri tıpkı bir polis gibi hata ve hile odaklı olmalıdır. Bu teori denetimde 1940'lar öncesine kadar büyük ölçüde geçerliliğini korumuştur. Denetimden geçmiş finansal tablolarda birçok muhasebe hilesinin ortaya çıkarılması ve yaşanan skandallar, teorinin yeniden tartışılmasına yol açmıştır. Finansal tabloların doğruluğu ve onaylanması konusunda denetimde yaşanan değişimleri açıklayamaması sebebiyle, teorinin açıklama gücünü büyük ölçüde yitirdiği anlaşılmıştır (Volosin, 2007, s.4). Denetimde %100 inceleme yerine örneklemeye

başvurulması ve finansal tablolar hakkında makul bir güvence sağlama yaklaşımının benimsenmesi, bu teorinin geçerliliğini kaybettiğini gösterir.

### 2.3.2. Borç kredibilitesi teorisi (Lending credibility theory)

Bu teori, denetimin birincil fonksiyonunun finansal tabloların güvenilirliğini artırmak olduğunu ileri sürer. Denetlenmiş finansal tablolar, yönetim (vekil) tarafından asilin yönetime olan güvenini artırmak ve bilgi asimetrisini azaltmak için kullanılır (Salehi, 2011, s.8378). Eğer hissedar, devlet ve yatırımcı gibi işletme paydaşları aldıkları bilgiye dayanarak bir yargıya varmak zorundalarsa, işletmenin ekonomik değerinin doğru olarak yansıtıldığına dair güvene sahip olmalıdırlar. Finansal tablo kullanıcıları güvenilirliğin artırılmasıyla birçok fayda elde ettiklerini idrak ederler. Örneğin, yatırımcılar güvenilir bilgiye dayandığı zaman, yatırım kararlarının kalitesinin arttığını algılarlar (Ittonen, 2010, s.4-5). Teorinin odak noktası, finansal bilginin güvenilirliğinin sağlanmasıyla, işletmenin daha kolay yatırımcı çekebileceği ya da borç bulabileceğidir.

### 2.3.3. Rasyonel beklentiler teorisi (Theory of rational expectations)

1920'lerde ve 1930'larda Amsterdam Üniversitesi'nden Profesör Theodore Limperg, Hollanda'da muhasebe ve denetim pratiklerini derinden etkileyen muhasebede yerine koyma maliyetleri hakkında bir teori geliştirmiştir. 1926 yılında ikinci Muhasebeciler Kongresi'nde Limperg, Güven Telkin Etme Teorisi (Theory of Inspired Confidence) olarak bilinen bir denetim kavramları setini de sunmuştur. Daha sonra bu teori, Rasyonel Beklentiler Teorisi olarak adlandırılmıştır (Soltani, 2007, s.8).

Teoriye göre denetim hizmetinin talep edilmesi, işletmeye dışardan paydaşların (üçüncü tarafların) katılımının direkt sonucudur. Bu paydaşlar işletmeye karşılıklı olarak katkı sağlayan hesap verebilirliği de talep ederler. Yönetim ve dışardan tarafların çıkarları arasında mümkün olabilecek farklılık, yönetim tarafından sağlanan bilgiye önyargıyla yaklaşılmasına neden olur. Bu yüzden bu bilginin denetlenmesi gerekir (Hayes vd., 2005, s.46; Salehi, 2011, s.8378).

Rasyonel Beklentiler Teorisine göre, denetçi rasyonel bir üçüncü tarafın beklentilerine ihanet etmeyecek şekilde denetim işini yürütür. Diğer taraftan, denetçi için hiçbir beklenti denetim yargısından daha önemli değildir (Limperg, 1985, s.18). Limperg'in teorisi, dinamik bir karakterdedir. Toplumun güvenilir finansal bilgi ihtiyacıyla denetçinin teknik yeterliliklerinin bu ihtiyaçları gidermesi arasında bağlantı

kurar. Toplumun ihtiyaçlarındaki değişimi ve denetim tekniklerine etkisini de dikkate alır. Bu teoriye göre toplumun ihtiyaçlarındaki değişim, denetim fonksiyonunun değişimine neden olur (Blokdijk vd., 1995:23).

Her iki teorideki benzerlikler ve vekâlet teorisindeki değişim dikkate alınırsa, Rasyonel Beklentiler Teorisi, Vekâlet Teorisinin daha erken ortaya çıkmış şekli olarak düşünülebilir (Duits, 2012, s.23).

### 2.3.4. Vekâlet teorisi (Agency theory)

Vekâlet Teorisi; muhasebede, ekonomide, finansta, pazarlamada, politik bilimlerde, örgütsel davranışta ve sosyolojide akademisyenler tarafından kullanılmıştır (Eisenhardt, 1989, s.57).

Vekâlet teorisi, vekâlet ilişkisinde meydana çıkabilen iki problemin çözümüyle ilgilidir. Birincisi vekâlet problemi, (a) asilin ve vekilin istekleri ve amaçları çatıştığında ve (b) vekilin asilin faaliyetlerini doğrulamasının çok zor veya pahalı olduğu durumlarda ortaya çıkar. Buradaki problem asilin, vekilin uygun şekilde davranıp davranmadığını doğrulayamamasıdır. İkincisi asil ve vekil riske karşı farklı tavırlara sahip olduklarında ortaya çıkan riskin paylaşılması problemidir. Buradaki problem, farklı risk tercihleri yüzünden asil ve vekilin farklı eylemleri tercih edebilmesidir (Eisenhardt, 1989, s.58).

Vekâlet teorisi, hem yönetim hem de üçüncü tarafların yararına olarak denetçinin görevlendirilmesini önerir. Bir işletme sözleşmeler ağı olarak görülür. Farklı gruplar (tedarikçiler, kreditörler, müşteriler, çalışanlar gibi) belirli bir fayda karşılığında, işletmeye çeşitli katkılar sağlarlar. Yönetimin görevi bu grupların ve sözleşmelerin düzenlenmesidir. Bu ilişkilerde yönetim, asilden (kreditörler, hissedarlar, çalışanlar gibi) katkı elde etmeye çalışan bir vekildir (Hayes vd., 2005, s.46).

En geniş kapsamlı kullanılan ve güncelliğini koruyan denetim teorisi, vekâlet teorisidir (Ittonen, 2010, s.5). Bu nedenle sonraki başlıkta denetime duyulan ihtiyaç, vekâlet teorisi açısından açıklanmıştır.

## 2.4. Denetime Duyulan İhtiyaç

Denetim iki ya da daha fazla taraf arasında bir arabulucu olarak denetçinin eylemleriyle yön verdiği bir değerlendirme sürecidir. Denetçi önceden belirlenen ölçütlere göre kanıtlar toplar, inceler, değerlendirir ve sonuçlarını ilgili taraflara raporlar. Denetimin ortaya çıkışı çoğu zaman vekâlet teorisi açısından değerlendirilmiştir. Buna

göre ekonomik kaynakların sahipleri (asli sermaye sahipleri) bu kaynaklar üzerindeki kontrolünü yöneticilere (temsilciler) devrettiklerinde bilgi asimetrisi ortaya çıkar. Eğer sahipler, tamamen kendi çıkarlarına göre hareket edebilecek olan yöneticiler üzerinde yeterli izleme gücüne sahip değillerse, yöneticilerin davranışları hakkında bağımsız tavsiyelerde bulunması için dışarıdan tarafların (denetçiler) yardımına ihtiyaç duyacaklardır (O'Regan, 2003, s.1).

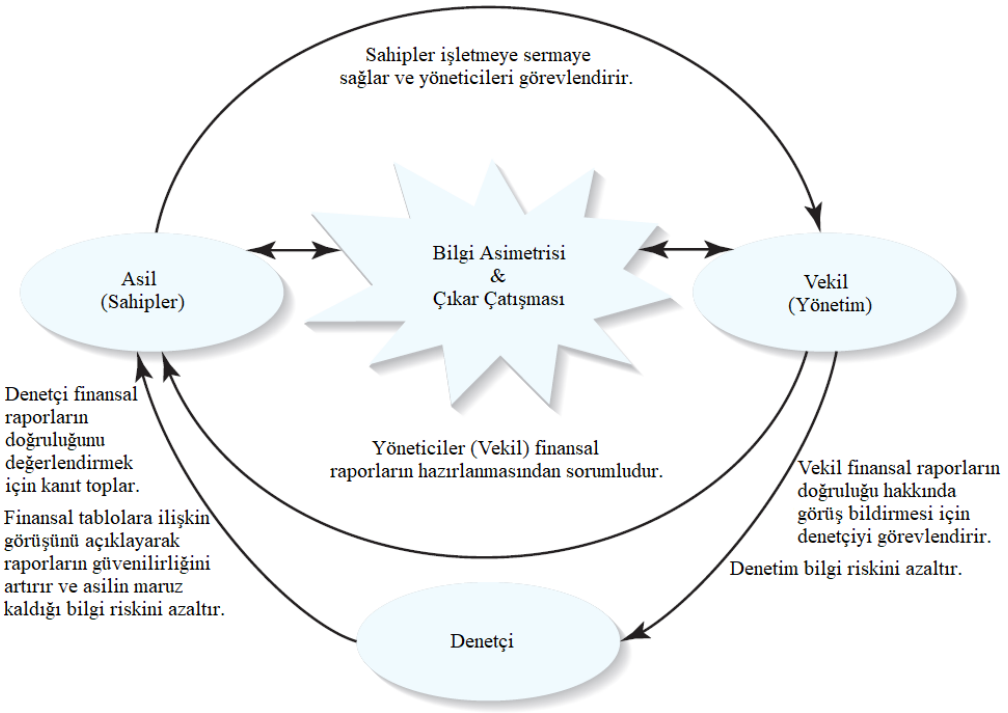
Vekâlet Teorisi literatürü, vekâlet problemini yaratan asil-vekil ilişkisinin iki yönünü ifade eder. Bunlardan ilki, yöneticilerin eylemleri açısından yöneticiler ve sahipler arasında önceliklerdeki uyuşmazlıktır. İkincisi, iki taraf arasında bilgi asimetrisine yol açan, sahiplerin yöneticilerin eylemleri üzerindeki kusursuz gözlemden yoksun olmalarıdır. Yönetici ve sahip arasında önceliklerdeki uyuşmazlıklar arttıkça ve yöneticinin eylemleri üzerinde sahiplerin gözetim gücü azaldıkça kayıpların artacağı varsayılır. Eğer ilişkilerinde iki taraf da sadece faydalarını en yüksek seviyeye çıkarmak için uğraşıyorlarsa, vekilin (yönetici) çoğu zaman asilin (sahip) çıkarlarına uygun hareket etmeyeceği su götürmez bir gerçektir (Jensen & Meckling, 1976, s.308).

Vekâlet Teorisi, yöneticinin işletmeye ait tüm bilgiye erişimi ve kontrolü olduğunun altını çizer. Bu durum, sahipler ve yöneticiler arasında bilgi asimetrisini doğurur. Bilgi asimetrisi, bağımsız bir denetçi tarafından üstlenilen bir rol olan bağımsız bir arabulucu ihtiyacını yaratır. Daha kesin bir ifadeyle, işletme yöneticisi tarafından hazırlanan finansal raporların doğrulanması ihtiyacı ortaya çıkar. Çünkü aksi durumda yöneticiler kendi finansal performanslarını manipüle etme imkânına sahip olacaklardır. Açık bir şekilde, işletme yönetimi işletmenin refahını artırmak için çalışan bir vekil olarak görülür. İşletme sahibi, yönetimin performansını değerlendirmek amacıyla finansal raporları kullanacağı için; finansal raporları üçüncü bir tarafın incelememesi, yöneticileri finansal performansı olduğu gibi yansıtmama yönünde teşvik eder. Yönetim kendi çıkarını gözeten davranışlar sergileyeceği için, işletme sahipleri böyle bir performans değerlendirmesini isteyecektir (Soltani, 2007, s.55).

Bağımsız bir denetçinin varlığı halka açıklanan yanlı bilginin miktarını sınırlayacağı için, vekâlet ilişkisinde denetime duyulan ihtiyacın haklılığını ortaya çıkarır. Bundan dolayı, vekâlet teorisi bilgiyi hazırlayan (yöneticiler) ve kullananlar (hissedarlar ve diğer ilgili taraflar) arasındaki çıkar çatışmasına karşı, denetçinin varlığını haklı gösteren tek sebep olmamakla beraber, denetim hizmetine ihtiyaç duyulması fikriyle

yakın ilişkilidir. İşletme içinde yürütülen izleme süreci, iç denetim ve kontroller ile bağımsız denetim tarafından üstlenilmelidir (Soltani, 2007, s.56).

Yönetim, kendi eylemlerinin sonuçlarını raporlamaktan sorumludur. İşletme sahipleri, bu süreci doğrudan gözlemleyemezler. Bu nedenle yönetim, raporları manipüle edebilecek bir pozisyona sahiptir. Sahipler, yönetimin raporları kendi çıkarlarına göre manipüle edeceğini varsayarak, yönetime ödenen bedelleri buna göre düzeltir. İşte bu noktada denetime olan ihtiyaç ortaya çıkar. Eğer yönetim dürüst ise, kendi faaliyetlerini izlemek ve sonuçlarını işletme sahiplerine raporlamak için bir denetçinin görevlendirilmesi, kendi menfaatleri açısından daha iyi olacaktır. Eğer yönetim işletme sahiplerinin sağladığı kaynakları kullanırken hesap verebilir olursa, sahipler işletmeye daha fazla yatırım yapmayı ve yönetime daha fazla ödemeyi kendi rızalarıyla isteyeceklerdir. Hesap verebilirliğin potansiyel etkisi, işletmeye yatırım yapanların sayısını ve sağlanan sermaye miktarını artırmaktır. Denetçinin rolü yönetim tarafından hazırlanan raporların sözleşme hükümlerine uygun olup olmadığını belirlemektir. Finansal bilginin denetçi tarafından doğrulanması, raporların güvenilirliğini artırır ve işletme yönetimi açısından yanlış ve yanıltıcı olmasını engelleyerek bilgi riskini azaltır. Bilgi riskinin azaltılmasının, hem sahiplere hem de yöneticilere birçok faydası vardır (Messier vd., 2016, s.6). Bu süreç Şekil 2.2'de özetlenmiştir.




**Şekil 2.2.** *Denetime Duyulan İhtiyaç (Messier, Glover, Prawitt, 2016, s. 7)*

Sermaye piyasalarının derinleşmesi ve çeşitli finansal araçların geliştirilmesi, gerçeğe uygun finansal bilginin önemini artırmıştır. İşletmelerin finansal tablolar aracılığıyla sağladığı bilgi, sadece ortaklar ya da çalışanlar gibi iç paydaşların değil, dünyanın her yerine yayılmış işletmenin çıkardığı menkul kıymetlere yatırım yapmayı düşünen potansiyel yatırımcıların da kararlarını etkileyecektir. Bu açıdan bakıldığında, işletmeye ait doğru bilgiye sadece yönetim-ortaklar arasındaki ilişkide ihtiyaç duyulmaz. İşletme tüm paydaşlarının kararlarını etkileyebilecek bilgiyi etkin finansal raporlama aracılığıyla ilgili taraflara iletmek zorundadır. Bu durum, denetime ihtiyaç duyan tarafların sayısını artırmıştır.

Temel fonksiyonu ekonominin ihtiyaç duyduğu sermayeyi tahsis etmek olan sermaye piyasalarının etkinliğinin temelinde, piyasada menkul kıymetlere ilişkin gerçekleşen fiyatların, o menkul kıymet ve onu ihraç eden şirkete dair tüm bilgileri yansıttığı kabulüne dayanan varsayım yatmaktadır. İdeal bir piyasada fiyatlar kaynak tahsisi için doğru işaretlerdir (Küçükkocaoğlu & Küçüksözen, 2005, s.161). Eugene Fama 1960'lı yıllarda hazırladığı doktora tezinde bu varsayımı Etkin Piyasa Teorisi olarak ortaya atmıştır. Piyasaların etkinliğinin ölçütü, piyasadaki bilgilere göre belirlenen bir finansal varlığın değerinin gerçek durumu yansıtabilme gücüdür. Fama'ya göre etkin piyasalar, rasyonel yatırımcının yatırım araçlarının gelecekteki değerini tahmin için rekabet ettiği ve önemli güncel bilgilere tüm kesimlerin özgürce ulaşabildiği piyasalardır (Fama, 1965, s.56).

Piyasalarda kullanıcıların bilgiye eşit oranda sahip olmaması, etkin piyasanın önündeki en büyük engeldir. Bu eşitsizlik asimetrik bilgi problemini yaratır. Bilgi asimetrisi, bir işlemin taraflarından birinin bilgiye sahipken, diğer tarafın bu bilgiden yoksun olmasıdır. Bilgi asimetrisi sorunu, ters seçim (advers select) ve ahlaki tehlikeye (moral hazard) yol açar. Asimetrik bilgi piyasada fon akımına engel olarak, üretken yatırım imkânlarının değerlendirilememesine neden olur (Hahm & Mishkin, 2000, s.22). Ters seçim, aslında yapılması rasyonel bir yatırımın bilgi asimetrisi nedeniyle eldeki eksik bilgiye dayanılarak yapılmaması ya da bunun tersi bir durumu ifade eder. Ahlaki tehlike ise, yine bilgi asimetrisi nedeniyle işlemin taraflarından birinin diğer tarafın ulaşamayacağı bir bilgiyi kendi menfaatleri doğrultusunda kullanması olasılığıdır.

Finansal piyasalarda bilgi asimetrisinin yarattığı ters seçim ve ahlaki tehlike gibi problemlerin ortadan kaldırılması için, her şeyden önce işletmelerin iyi işleyen bir finansal raporlama sistemine sahip olmaları gerekir. Finansal raporlamanın en genel

amacı yatırım, kredi ve benzer konularda finansal bilgi kullanıcılarına faydalı bilgiler sağlamaktır. Finansal bilginin karar almada faydalı olabilmesi için anlaşılabilir, ilgili ve güvenilir olması gereklidir (Cemalcılar & Önce, 1999, s.32).

Finansal raporlamanın ilgili rapor kullanıcılarının güvenini tesis eden tamamlayıcı unsuru denetimdir. Ancak bağımsız bir denetçi tarafından verilen denetim hizmetiyle, yatırımcıların ve diğer rapor kullanıcılarının işletmenin açıkladığı finansal bilgiye olan güveni sağlanabilecektir. Denetim hizmeti, işletmenin sunduğu finansal bilginin güvenilirliğini onaylayarak asimetrik bilgi riskini azaltır ve böylece işletmenin karlılığını ve kar dağıtım beklentilerinin gelişimini değerlendiren yatırımcıların, mevcut ve potansiyel hisse senedi yatırımlarını işletmeye çeker (Ashbaugh & Warfield, 2003: 4).

Makro açıdan bakıldığında da, finansal raporlamadan elde edilen bilginin doğruluğunun bağımsız denetim mekanizmasından geçmesi, sermaye piyasalarına olan güveni artırarak piyasaların derinleşmesine ve bilgi asimetrisinden kaynaklanan sorunları azaltarak –ancak bu şekilde üretim ve yatırım kararları daha rasyonel verilebilir- ulusal çapta ekonomik kalkınma hedeflerine ulaşılmasına katkı sağlayacaktır.

### 2.5. İç Denetim Tanımı

IIA, kurulduğu günden bu yana iç denetim tanımı üzerinde, değişen işletme çevresi ve gelişen yeni ihtiyaçlara mesleğin cevap verebilmesini sağlamak amacıyla değişiklikler yapmıştır. Aslında iç denetçilerin güncel koşullara göre yürüttükleri hizmetin özlü bir ifadesi, IIA'nın yapmış olduğu tanımlarda gizlidir. IIA'nın yapmış olduğu en son tanım şöyledir (IIA, 2010a, s.5);

*"İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur."*

Tanım bileşenlerine ayrılarak daha iyi anlaşılabilir.

***Bağımsızlık ve objektiflik***: Hem IIA'nın etik kodları hem de Uluslararası İç Denetim Standartları, bağımsızlık ve objektifliğin iç denetim uygulamalarındaki önemini vurgular. Bağımsızlık, iç denetim biriminin örgütsel statüsünü yansıtırken, objektiflik ise iç denetçilerin bireysel mental davranışlarında tarafsızlığını ifade eder. Bağımsızlık, objektifliği veya objektif görünmeyi tehdit eden şartlara karşı özgür kalabilmektir. Denetçi faaliyetlerinde objektifliğine karşı ortaya çıkan tehditleri yönetebilmelidir.

Denetim sözleşmesi ve iç denetimin fonksiyonel ve örgütsel durumu, bağımsızlığı koruyacak şekilde düzenlenmelidir. Objektiflik, iç denetçilerin denetim işini yürütürken, denetim kalitesinden önemli tavizler vermeden ve dürüst bir inançla sorumluluklarını üstlenmesini sağlayan önyargısız mental bir tavırdır. Objektiflik, denetçinin denetim konuları üzerindeki yargısını başkalarından etkilenmeden oluşturmasını gerektirir. (Reding vd., 2013, s.1-5).

İç denetçilerin iç denetim hizmetini yürütürken bağımsızlık ve objektifliklerini kaybetmeleri, iç denetim faaliyeti ve denetim görüşünü olumsuz etkileyen en önemli etkendir. Kültürel, ırksal ve cinsiyet önyargıları, ekonomik ve kişisel ilişkiler, sosyal baskı ve denetçinin iç denetim süreçlerine olan aşinalığı bağımsızlık ve objektifliği etkileyen temel faktörler olarak sıralanabilir (Chapman & Anderson, 2002, s.34-37).

***Organizasyonun amaçlarına ulaşmasına yardım etme***: İç denetimin görevleri organizasyonun kurumsal amaçlarına yönelik olarak sağlam bir şekilde düzenlenir. Organizasyonu başarıya ulaştırmanın anahtarı, kurumsal yönetim (Kötü yönetilen işletmeler başarılı olmazlar), risk yönetimi (Amaçlara ulaşılması için riskler, temel odak noktası olmalıdır) ve iç kontrollerdir (İç kontroller amaçlara ulaşılmasını garanti edecek şekilde düzenlenmelidir). Ayrıca iç denetçiler, işletmelerini uzun dönemli kurumsal başarı için gerekirse iç denetim faaliyetini dış kaynak kullanarak yürütme alternatifine yönlendirmeli ya da denetim ekiplerini bu doğrultuda geliştirmelidir (Pickett, 2011, s.133).

***Sistematik ve disiplinli bir yaklaşım***: İç denetim günümüzde tamamen gelişmiş bir meslek haline gelmiştir. İç denetim açık bir mesleki standartlar setine sahiptir ve denetim işi hizmet kalitesini artırmak için kullanılan en iyi uygulamalar rehberlerine göre yürütülebilir. Bu profesyonelliğin bir ölçüsü olarak, işletmeler denetçilerinden işlerini sistematik ve disiplinli bir yaklaşımla yerine getirmelerini beklemektedir. Bir işletmede faaliyetleri geliştirmek ve onlara değer katmak için, iç denetim süreci sistematik ve disiplinli bir şekilde yürütülmelidir.

***Faaliyetleri geliştirme ve değer katma***: Denetim, işletmenin ihtiyaçlarını anlamaya çalışan müşteri tabanlı bir hizmettir. Denetim hizmeti, işletme için belirlenen faydaların sağlanmasına yönelik olarak yürütülmelidir. İşletme faaliyetlerine değer katma, iç denetim yöneticisinin en başta gelen temel düşüncesi olmalıdır. Denetim süreçlerinin tamamı, bu temel düşünceyle yönetilmelidir.

***Güvence ve danışmanlık faaliyetleri***: İç denetim tanımı incelendiğinde, iç denetim faaliyetinin güvence ve danışmanlık şeklinde iki temel işlevi olduğu görülür. Güvence sağlama, iç denetimin öncelikli işlevidir. Güvence sağlama, işletmenin risk yönetimi, kontrol ve yönetişim süreçlerine dair bağımsız bir değerlendirme sağlamak amacıyla kanıtların nesnel bir şekilde incelenmesidir. İç denetçinin bir kurum, faaliyet, işlev, süreç, sistem veya bir başka unsur hakkında bağımsız görüş veya kanaat sunabilmek için elindeki kanıtları nesnel bir şekilde değerlendirmesidir. Danışmanlık hizmetleri ise; herhangi bir idari sorumluluk üstlenmeden bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı denetlenen ile birlikte kararlaştırılan istişari faaliyetler ve bununla bağlantılı diğer hizmetlerdir. Usul ve yol göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek; bu kapsamdaki faaliyet örnekleridir (Uzun, 2012, s.79-80).

## 2.6. İç Denetime Duyulan İhtiyaç

Bir işletmede iç denetim faaliyetinin varlığına duyulan ihtiyaç, genel olarak aşağıdaki başlıklar altında özetlenebilir.

### 2.6.1. Sorumluluk ve hesap verebilirlik

Çağdaş işletme yönetiminde yöneticilerin yetki ve sorumluluklarını işletme çalışanlarına devretmesi bir mecburiyettir. Üst yönetimin çalışanlarının görev ve sorumluluklarını istenildiği şekilde yerine getirip getirmediklerini öğrenmesi gerekir. İşletme yönetimi, hem üzerindeki yoğun iş yükü hem de çalışanlarla arasındaki çıkar çatışması nedeniyle bu bilgiye gerektiği gibi ulaşamaz. İç denetçiler, bu görevi yöneticilerin yerine, iç denetçilik mesleğinin gerektirdiği bilgi toplama, analiz etme ve problemi ortaya çıkarma konusundaki uzmanlıklarıyla yerine getirirler. İşletme içinde çalışanların hesap verebilirliği, iç denetim sayesinde istenilen seviyelere getirilebilir.

### 2.6.2. Vekâlet ilişkisi

İşletme sahipleri, yöneticilerin görevlerini gerektiği gibi yerine getirip getirmediği konusunda araştırma yapacak teknik bilgi ve zamana sahip değildir. Yöneticiler daha fazla ücret almak gibi kendilerine daha fazla menfaat sağlamak amacıyla hareket edebilirler. Bu nedenle, işletme sahiplerinin yöneticilere emanet ettikleri kaynakların etkin ve verimli kullanımı konusunda şüpheleri oluşabilir. Vekili olarak işletmeyi yöneten

yöneticiler hakkında, işletme sahiplerinin şüphelerini gideren en önemli kontrol mekanizması iç denetimdir. İç denetçiler finansal ve finansal olmayan faaliyet ve olayları denetleyerek, işletme sahipleri ve yöneticiler arasındaki potansiyel çıkar çatışmasının önüne geçerler (Kurnaz & Çetinoğlu, 2010, s.27-28).

### 2.6.3. Tasarruf ihtiyacı

İç denetim, işletme faaliyetlerinin daha verimli hale getirilmesi için incelemeler yapar ve faaliyetlerin daha etkin ve verimli yürütülmesi amacıyla ölçütler geliştirir. İç denetim, tespit ettiği eksiklikleri gidererek, işletmenin büyük tasarruflar elde etmesine olanak tanır. İç denetimin ortaya çıkardığı ve önüne geçtiği maddi kayıplar, çoğu zaman iç denetim biriminin yıllık maliyetinden daha fazladır (Akarkarasu, 2000, s.13).

### 2.6.4. Hileli işlemlere karşı korunma ihtiyacı

Halka açık işletmelerde küçük pay sahiplerinin kar payı alma gibi ortaklık haklarına zarar veren en büyük etken hileli işlemlerdir. Bu hileli işlemlerin tipik örneği halka açık işletmelerde büyük pay sahiplerinin sahip oldukları diğer işletmelere, küçük pay sahipleri ve işletmenin zararına olarak, işletme kârının örtülü olarak aktarılmasına yönelik yapılan işlemlerdir. Diğer taraftan, işletme çalışanlarının yaptığı varlıkların çalınması ya da kötüye kullanılması şeklinde ortaya çıkan hileler, işletmeye ve dolaylı olarak pay sahiplerinin haklarına zarar vermektedir. İşletmede hileli işlemlere engel olacak etkin işleyen kontroller geliştirilmesi gerekir. İç denetim, geliştirdiği kontrollerle işletmede hem hileden hem de çalışanların hatalarından kaynaklanan kayıpların önüne geçer ve menfaat sahiplerinin haklarını korur.

### 2.6.5. Yönetime danışmanlık ve yardım

Günümüzde iç denetim, işletme yönetiminin en büyük yardımcısı haline gelmiştir. İç denetimin danışmanlık işlevi, hem iç denetim tanımında hem de iç denetim standartlarında vurgulanır. İç denetim, yönetimin ihtiyaçlarını gidermek için çalışır. İç denetçiler kendi planlarını ve faaliyetlerini yönetimin ve işletmenin amaçlarına göre düzenlerler. İç denetçiler yönetimin örgütsel başarı için en çok önem verdiği alanlarda mümkün olan en yüksek değeri üretmek amacıyla pozisyon alırlar. Örneğin yönetim karar alma süreçlerinde iç denetimden büyük ölçüde faydalanır. İç denetçiler, karar almak için

gerekli olan veriyi elde eder ve geçerliliğini araştırır. Yönetim tarafından alınan kararların etkilerini değerlendirir ve yönetimin öngöremediği riskleri ortaya çıkarır.

## 2.7. İç Denetimin Tarihsel Gelişimi

İç denetimin tarihi, Pers İmparatorluğu'na kadar uzanmaktadır. İç denetimden ilk defa, ülkesini milattan önce 521-425 yılları arasında yöneten ilk Pers Kralı Darius zamanında faydalanıldığını kabul eden bazı iddialar vardır. Krallar kralı Darius, yılın farklı zamanlarında bulunduğu, ülkesinin farklı yerlerindeki dört başkentinden (Persepolis, Hagmatana, Susa, Tizpon) imparatorluğunu yönetirdi. Ülkesini yirmi eyalete bölmüştü ve her biri eyaletinin refahına göre imparatorluğa vergi ödeyen pers valileri tarafından idare ediliyordu. Darius, yasalarının valileri tarafından dürüstçe uygulanmasını sağlamak için imparatorluğunun her bölgesine temsilcilerini yollardı. Kralın gözleri ve kulakları olarak bilinen bu temsilciler, büyük olasılıkla tarihteki ilk iç denetçilerdi (Murray, 1976, s.98).

İç denetim çok eski dönemlerde ortaya çıkmasına karşın, 19. yüzyılda sanayi devrimi sonucunda büyük ölçekli üretim sistemlerinin gelişmesi, tutarlı üretimin yapılması ve kalitenin öneminin anlaşılmasıyla devam eden sürece kadar, önemli bir gelişim gösterememiştir. 20. yüzyılda yönetim teorileri ve pratiklerinin gelişmesiyle yönetimin kurumsal faaliyetlerdeki belirgin rolünün anlaşılması, mesleğin gelişimini hızlandırmıştır (Pitt, 2014, s.4).

20. yüzyılın ilk yarısında, iç denetçiler öncelikli olarak finansal hata ve düzensizliklerin bulunması ve muhasebe kayıtlarının doğrulanmasından sorumluydu. Ayrıca daha az da olsa dış denetçilere yardım edilmesi ve onların izlenmesini üstleniyorlardı. İç denetçilerin statüleri hakkında çalışmalar yapan Walter Meigs'in gözlemlerine göre, 1930'larda iç denetçiler ya rutin olarak muhasebe belgelerindeki büro işlerinden kaynaklanan hataların sürekli olarak araştırılması görevine atanmışlardı ya da farklı bölgelere dağılmış şubelere sahip olan işletmelerde temsilci olarak sürekli seyahat etmektelerdi. İlk iç denetçiler, rutin muhasebe doğrulamalarını üstlenerek büro işlerine yardım eden destek personeli olarak görev yaparlardı. İç denetimin bu eski şeklinin izleri, 1970'lerin başına kadar bazı işletmelerde varlığını sürdürdü. 1960'ların sonuna kadar birçok perakende işletmesinde iç denetçiler, iş gününün sonunda yazar kasa kayıtlarını kontrol eden kişilerdi (Moeller, 2009, s.5).

1941 yılında Uluslararası İç Denetçiler Enstitüsü (IIA), kendi işletmelerinde iç denetçi unvanına sahip kişiler tarafından sadece 24 üyeyle Amerika'da kuruldu. IIA'nın kurucularının amacı, bu yeni mesleki alanda hem deneyimlerini paylaşmak hem de diğerlerinin deneyimlerinden yeni bilgiler elde etmekti. Böylece meslek doğdu ve geçen yıllar boyunca birçok değişiklik geçirdi. IIA, 1947 yılında İç Denetimin Sorumlulukları Raporunu (Statement of Responsibilities of Internal Auditing) yayınladı. Bu rapor iç denetimin öncelikli olarak muhasebe ve finansal konularla ilgilenmesi gerektiğinin ancak haklı olarak faaliyetle ilgili konularla da ilgilenebileceğinin altını çizer. Diğer bir ifadeyle bu rapora göre, iç denetimin asli görevi muhasebe ve finansal konulardır, fakat diğer faaliyetler de iç denetçiler için meşru hedeflerdir (Pitt, 2014, s.4).

1957 yılında IIA, İç Denetimin Sorumlulukları Raporunu dönemin ihtiyaçlarına göre yeniden incelemiş ve önemli değişiklikler içeren halini yayınlamıştır. Rapor, iç denetçilerin yönetime aşağıda sıralanan hizmetleri sunmasına izin verir (Ramamoorti, 2003, s.5):

- Finansal, operasyonel ve muhasebe kontrollerinin sağlamlığı ve yeterliliğini inceleme ve değerlendirme.
- Belirlenen politikalar, planlar ve yordamlara uygunluğun seviyesini belirleme.
- İşletme varlıklarının muhasebeleştirilmesi ve her türden kayba karşı korunma seviyesini tespit etme.
- İşletme içinde geliştirilen muhasebe verilerinin ve diğer verilerin güvenilirliğini tespit etme.
- İşletmede yüklenilen sorumluluklar yerine getirilirken performans kalitesini değerlendirme.

Modern iç denetim mesleği, değişen işletme dünyasının ihtiyaçlarına göre yıllar itibarıyla köklü değişiklikler göstermiştir. İç Denetimin Sorumlulukları Raporu, IIA tarafından denetim mesleğinde yaşanan hızlı değişim sebebiyle, 1976, 1981 ve 1990 yıllarında büyük çaplı revizyonlar geçirmiştir. Geçmişte sunmadığı birçok yeni hizmet, günümüzde iç denetim faaliyetinin kapsamına girmiştir. İşletme dünyasında sürekli devam eden değişim ve ortaya çıkan yeni gereksinimler, iç denetimin yeni sorumluluklar üstlenmesini kaçınılmaz hale getirmektedir.

Modern iç denetim mesleğinin ortaya çıktığı dönem olan 1940'ların işletme dünyası, iç denetçiler için bugüne göre çok farklı bir yetenekler setini gerektirmekteydi. Örneğin, laboratuvar ortamındaki birkaç elektro-mekanik cihaz ve faaliyet dışında, dijital

bilgisayar sistemleri yoktu. Bilgisayarlar kayıt saklama ve diğer hesaplama ve muhasebe işlemleri için kullanışlı hale gelmeye başlayana kadar, işletmeler bilgisayar programlarına ihtiyaç duymadılar. Benzer şekilde, işletmeler çok ilkel telefon bağlantılarına sahiplerdi; gelen bütün çağrılar santral personeli tarafından sınırlı sayıdaki masaüstü telefona yönlendiriliyordu. Günümüzde, hepimiz otomatikleştirilmiş dünya çapında bir telekomünikasyon ağı ve internet ile birbirimize bağlıyız. Modern işletmelerde ve diğer kurumlarda artan karmaşıklık iç denetçilerin çeşitli işletme kontrollerinde uzmanlaşmaları ihtiyacını yaratmıştır. Eğer günümüzde, geçmişe göre değişen şartları ve bu değişimin yarattığı farklı ihtiyaçları değerlendirirsek, iç denetimin niteliğini daha iyi anlayabiliriz (Moeller, 2009, s.6).

### 2.8. İç Denetimin Kapsamı ve Amaçları

İç denetimin amacı, incelediği faaliyetlerle ilgili analizler, değerlendirmeler, tavsiyeler ve yorumlar getirerek işletmenin tüm çalışanlarına sorumluluklarını etkili bir şekilde yerine getirmelerinde yardımcı olmaktır. İç denetçi, işletme faaliyetlerinin her aşamasıyla ilgili olarak yönetime hizmet sunabilir. İç denetim faaliyeti yönetime hizmet sunmak amacıyla, finansal ve finansal olmayan tüm işletme faaliyetlerini içine alır. İşletme faaliyetlerinin tüm yönleriyle anlaşılması amacı, finansal kayıtların ötesinde bir incelemeyi kapsar (Fadzil vd., 2005, s.847).

İç denetçiler, işletme içinde çeşitli faaliyetler ve kontrollere ilişkin sistematik ve objektif değerlendirme yapmaktan sorumludur. İç denetim biriminin amaçları işletmenin yapısına ve büyüklüğüne, yönetimin ve yönetişimden sorumlu olanların isteklerine ve gereksinimlerine bağlı olarak değişir. Genel bir bakış açısıyla, iç denetim faaliyetinin temel amaçları (Ducu, 2013, s.112):

- Tatmin edici düzeyde operasyonel ölçütlere ulaşılması,
- İşletmenin risklerinin tespit edilmesi ve ortadan kaldırılması,
- Yasal düzenlemelere, işletmenin politika ve yordamlarına uyum gösterilmesi,
- İşletmenin amaçlarına etkin ve verimli bir şekilde ulaşması,
- Kaynakların etkin ve rasyonel şekilde kullanılması, olarak sıralanabilir.

İç denetimin asıl amacı, işletmeye değer katmak amacıyla denetim faaliyetlerini sürdürmek ve çalışanların görevlerini etkin bir şekilde yerine getirmelerine yardımcı olmaktır. İç denetim, uygun bir maliyetle amaçlarına ulaşmalı ve işletmede etkin bir iç kontrolü teşvik etmelidir (Kell, vd., 1989, s.801). İç denetçilerin etkin bir şekilde yerine

getirmekle görevli oldukları başlıca iç denetim faaliyetleri (Yılancı, 2003, s.9; Özeren, 2000, s.2; Uzay, 2003, s.210):

- "Muhasebe kontrollerinin ve yönetsel kontrollerinin yeterliliğini ve uygulanmasını gözden geçirip değerlemek ve işletme içinde uygun maliyetle etkin iç kontrolü geliştirmek,
- Finansal ve operasyonel bilgilerin kaydedilmesi, sınıflandırılması, ölçülmesi ve raporlanmasında kullanılan yöntemlerin doğruluğunu araştırmak,
- İşletme faaliyetlerinin önceden belirlenmiş politika, yordam, plan ve yönergelere uygunluğunu araştırmak,
- İşletme faaliyetleri ve raporları üzerinde etkileri olan politika, yordam, kanun ve düzenlemelere uygunluğu sağlamak amacıyla oluşturulan sistemleri incelemek ve ihtiyaç duyulduğunda geliştirmek,
- İşletme varlıklarının her türlü zarara karşı korunup korunmadığını araştırmak ve varlıkların korunmasını sağlayıcı tedbirler geliştirmek,
- Yönetimin düzenleyip sunduğu her türlü bilginin doğruluk ve güvenilirliğini araştırmak,
- İşletmede iç denetim ile ilgili tüm politika ve süreçleri yazılı hale getirmek,
- Denetim raporunda sunulan tavsiyelerin ve eylem planlarının uygulanıp uygulanmadığını takip etmek,
- Risk yönetimi süreçlerinin geliştirilmesine destek olmak, işletmede uygulanan risk yönetimi metodolojisinin sektördeki en iyi uygulamaları sağlayacak yetkinlikte olup olmadığını değerlendirmek amacıyla sektörel ve kurumsal her türlü bilgiyi değerlendirmek,
- İç denetim standartları, süreçleri ve teknikleriyle ilgili gelişmeleri sürekli takip etmek ve iç denetim faaliyetleriyle ilgili bilgi ve tecrübenin artırılması için çaba göstermek,
- Yolsuzluk eylemlerini takip etmek amacıyla, yolsuzluğun önlenmesi konusunda araştırma yapmak ve işletmede yolsuzluğu önlemeye yönelik kontrolleri incelemek ve geliştirmek,
- Bağımsız denetçilerle iletişimi ve koordinasyonu sağlamak, iki taraf açısından da uygun görüldüğünde işbirliği yapmak,
- İşletmenin amaçlarıyla uyumlu olarak iç denetim biriminin amaçlarını tanımlamak ve ulaşılması için çaba göstermek,
- İşletme faaliyetlerinin kalitesini araştırmak ve faaliyetlerle ilgili gerekli iyileştirme önerilerini yönetime raporlamaktır. "

## 2.9. İç Denetim Hizmetleri

İç denetimin rolü çok geniştir. Risk yönetimi, kontrol ve yönetişim süreçlerinin geliştirilmesi kapsamında, bir işletmeye değer katmak için üstlenilen işin türü büyük ölçüde değişkenlik gösterir. Örneğin, suistimallerin yaygın görüldüğü bir sektörde, işletmelerin katı yasal düzenlemelere uyum sağlama ihtiyaçlarını karşılayarak işletmeye değer katmanın en makul yolu, uygunluk incelemeleri yapmaktır. Ya da yeni ürünler

sunma konusunda hızlı olmanın anahtar başarı faktörü olduğu, hızla büyüyen sektörlerdeki işletmeler için, projeler ve kontrol programlarını geliştirmeye yönelik olarak danışmanlıkta bulunulması ya da öneriler sunulması, işletme faaliyetlerine değer katma açısından en uygun iç denetim hizmeti olacaktır. Diğer taraftan, gelişmekte olan ülkelerdeki kamu kurumları, iç denetim çabalarının yolsuzluk problemleriyle uğraşmaya ve en iyi kontrollerin düzenlenmesine yardım etmeye yönelik olarak yönlendirilmesini isteyebilirler. Veya uzun dönemli bir reform programına kalkışan işletmeler ve kamu kurumları, iç denetçilerinden değerlendirme programlarını kolaylaştıran risk değerlendirme yeteneklerinin ve uygun iç kontrollerin geliştirilmesine yardım etmelerini isteyebilirler. Dünyanın çeşitli bölgelerinde örgütlenmiş iştirakler, ortak girişimler ve ortaklık anlaşmalarıyla bağlı organizasyonlar ise, iç denetçilerinin yerel şubeler, anlaşmalar ve riskin doğru yönetilip yönetilmediği hakkında genel merkezi bilgilendirmelerini isteyebilirler.

İç denetim hizmetleri, şartlara ve içeriğe bağlı olarak tamamen değişkenlik gösterir. Kurumsal yönetişim düzenlemelerine odaklanan iç denetim firmaları, kendilerine teklif edilen bir işi hemen üstlenmek yerine, işe ilişkin en iyi yönlendirmeleri yapmaya çalışacaklardır. Bunu kolaylaştıran iç denetim yönetmeliğidir. Yönetmelikte, işletme tarafından belirlenen başarı ölçütleri, içeriği oluştururken; temel parametre mesleki standartlardır. Denetçinin teklif ettiği denetim hizmetleri, bu ölçütlere bağlı olarak değişir. Aşağıda sıralanan hem kamu kurumlarına hem de özel sektör işletmelerine sunulabilecek iç denetim hizmetleri, çeşitli iç denetim firmalarının internet sitelerinden elde edilmiştir. Denetim firmasından beklenen, işin içeriği ve kapsamına göre listelenen hizmetlerden biri ya da bir kaçını iç denetim faaliyetinin kapsamına almasıdır (Pickett, 2010, s.335):

- "Döngü denetimi (Stoklar ve maliyet döngüsü, satın alma ve ödemeler döngüsü),
- Kasa, stoklar ve muhasebe kayıtlarının ani denetiminin yapılması,
- Varlık kayıtlarının, stokların ve uygulanan güvenlik politikalarının doğrulanmasıyla varlıkların ve bilginin korunması,
- Spesifik problemlerin araştırılması,
- Yönetimin taleplerine yanıt verilmesi,
- Operasyonel etkinlik ve verimliliğin incelenmesi,
- İç kontrolün incelenmesi,
- Hile araştırmaları,
- Gelirlerin, sözleşmelerin ve operasyonel harcamaların üzerindeki kontrollerin incelenmesi,

- Hile, israf ve kötüye kullanım iddiaları için irtibat noktaları geliştirme,
- Bilgi sisteminin incelenmesi,
- Finansal ve uygunluk denetimi,
- Performans denetimi,
- İç kontrolü inceleyerek zayıf alanların test edilmesi,
- Raporlama usulsüzlüklerinin denetimi,
- Varlıklara ilişkin doğrulamalar yapma ve varlıkların korunmasıyla ilgili tedbirlerin incelenmesi,
- Raporlama sistemlerinin ve yordamlarının değerlendirilmesi,
- Maliyet tasarrufu hakkında incelemeler,
- Muhasebe kontrollerinin ve yönetsel kontrollerin incelenmesi,
- Finansal ve performans denetimi,
- Teknik destek ve performansla ilgili problemler ve maliyet tasarrufuyla ilgili yönetimin çalışmalarının incelenmesi,
- Projelerle ilgili özel incelemeler,
- Çevresel denetimler (Environmental audits),
- Yönetim süreçlerinin değişiminin denetimi,
- Faaliyet denetimi,
- Bilgi teknolojileri denetimi,
- İç kontrol hakkında personele rehberlik edilmesi,
- İşletmeye değer katan tavsiyelerde bulunulması,
- İşletme süreçlerinin analiz edilmesi,
- Risk değerlendirme,
- Kalitenin incelenmesi ve artırılması,
- Amaçlara ulaşılması için geliştirilen mekanizmaları güçlendiren tedbirler almak,
- Kurumsal yönetişim süreçlerinin değerlendirilmesi,
- Risk yönetimi pratikleri hakkında yönetimle birlikte çalışmak,
- Problemlerin giderilmesi için önlemler alma ve maruz kalınan riskler hakkında tavsiyelerde bulunma,
- Risk yönetimi düzenlemelerini inceleme,
- Yönetimin uygulamalarını destekleyen pratik çözümler üretme,
- Büyük bilgi sistemi projelerine katılma,
- Yönetim süreçlerinin kalitesini artırma,
- Muhasebe ve finansal raporlama sisteminin denetimi,
- Yasalar, düzenlemeler, politikalar ve yordamlara bağlılık hakkında uygunluk denetimi – Uygunluğu sağlamaya yönelik kontrollerin geliştirilmesine odaklanır,
- Geliştirilme aşaması boyunca bilgi teknolojilerinin denetimi,
- Yordamları değiştirirken yönetime tavsiyeler sunma,
- İşletmede risk ve kontrol farkındalığını artırma,

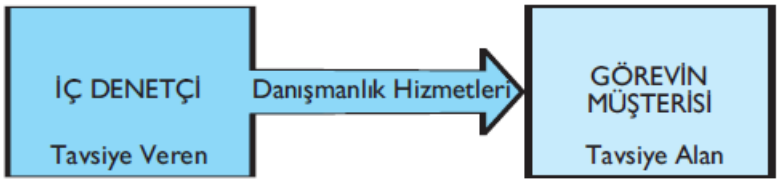
- İç kontroller hakkında bağımsız güvence verme,
- Kontrolle ilgili sorunlar hakkında rehberlik etme ve genel tavsiyelerde bulunma,
- Yönetimle tartışarak denetim yaklaşımının belirlenmesi ve bunun sonucunda iç denetimin ayrıcalıklı yapısının oluşturulması,
- İç denetim tavsiyeleri sonucunda hazırlanan eylem planlarının değerlendirilmesi,
- Bağımsız denetim ile ortak projeler yürütülmesi ve iletişimin geliştirilmesi,
- Yönetim tarafından istendiğinde özel projelere katılma ve rehberlik etme,
- Yeni ve mevcut sistemlerin, programların ve yordamların incelenmesi,
- Kontrol bilinciyle ilgili seminerler verme,
- Maliyet etkin kontrol sistemlerinin kurulması için tavsiyeler getirme,
- Finansal bilgi ve raporlama sonuçlarını izleme,
- Duran varlıklar, ödeme makbuzları, bütçeler, satın almalar ve diğer muhasebe rutinlerinin incelenmesi,
- E-ticaret düzenlemeleri ve güvenliğinin incelenmesi,
- Hesap verebilirlik ve hile farkındalığı hakkında eğitimler verilmesi. ”

IIA'nın yaptığı iç denetim tanımı, tarihsel süreç içerisinde ortaya çıkan ihtiyaçlar ve bu ihtiyaçların iç denetçilere yüklediği yeni sorumlulukları ifade etmek amacıyla değişim göstererek son halini almıştır. Tanımda da ifade edildiği üzere, iç denetim kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini geliştirmeye yönelik olarak, işletme yönetiminin sorumluluğunda olan hemen hemen her konuya çözüm üretmek üzere, çok geniş bir çerçevede hizmet sunmaya çalışır. Ancak iç denetçilerin sunduğu hizmetler; güvence hizmetleri ve danışmanlık hizmetleri olarak iki ana kategoriye ayrılabilir (IIA, 2010a, s.3);

Güvence hizmetleri, iç denetçinin, bir süreç, sistem veya başka bir konu hakkında bağımsız görüş veya kanaat sunabilmek için, eldeki kanıtları objektif bir şekilde değerlendirmesini içerir. Güvence görevlerinin nitelik ve kapsamı iç denetçi tarafından belirlenir. Güvence hizmetlerinin, genellikle, üç tarafı vardır: (1) Süreç, sistem veya ele alınan diğer bir konunun doğrudan içinde olan kişi veya grup (süreç sahibi; denetimin faaliyet alanını oluşturan, denetlenen taraf), (2) Değerlendirmeyi yapan kişi veya grup (iç denetçi), (3) Değerlendirmeyi kullanan kişi veya grup (kullanıcı; denetim sonuçlarının iletileceği taraf). Güvence hizmetinin tarafları Şekil 2.3'te sunulmuştur.


**Şekil 2.3.** *Güvence Hizmetinin Tarafları (Uzun, 2012, s. 80)*

Danışmanlık hizmetleri, doğası gereği tavsiye niteliğinde olup genellikle görevlendirmeyi talep eden müşterinin özel talebi üzerine gerçekleştirilir. Danışmanlık hizmetlerinin nitelik ve kapsamı, değerlendirmeyi talep eden müşteriyle iç denetçi arasındaki sözleşmeye tabidir. Danışmanlık hizmetlerinin genellikle iki tarafı vardır: (1) Tavsiye veren kişi veya grup (iç denetçi), (2) Tavsiye talep eden ve alan kişi veya grup (görevin müşterisi). İç denetçi danışmanlık hizmeti verirken, objektifliğini muhafaza etmeli ve idarî sorumluluk almamalıdır. Danışmanlık hizmetinin tarafları Şekil 2.4'te gösterilmiştir.




**Şekil 2.4.** *Danışmanlık Hizmetinin Tarafları (Uzun, 2012, s. 80)*

Daha önce de örnekleri verildiği üzere, çok sayıda iç denetim hizmeti vardır. İç denetçiler tarafından sunulan hizmetlerin listesi, genel olarak, güvence ve danışmanlığın geniş sınıflandırmasına dâhil edilebilir. Güvence ve danışmanlık hizmetleri, birbirlerini tamamlayıcı oldukları gibi araştırma ve denetim dışı görevler gibi, başka denetim hizmetlerinin de iç denetçi tarafından üstlenilmesini engellemez. Ayrıca birçok denetim hizmetinin hem güvence hem de danışmanlık yönü olabilir (IIA, 2010a, s.42).

## 2.10. İç Denetimin Türleri

Çok geniş bir faaliyet alanına sahip olan iç denetim, beş temel denetim uygulamasını kapsar. Bu denetim uygulamaları; mali (finansal) denetim, uygunluk denetimi, performans (başarım) denetimi, sistem denetimi ve bilgi teknolojileri denetimidir (Alptürk, 2008, s.22).

***Mali Denetim***; mali raporlardaki verilerin, denetlenen birimin varlık ve yükümlülüklerinin gerçek değeriyle, finansman kaynaklarıyla, varlıklarının yönetimiyle ve tahsis edilen bütçe ödenekleriyle uyumlu olup olmadığının değerlendirilmesidir.

***Uygunluk Denetimi***; işletmenin tamamının veya bir biriminin mali işlemlerinin ya da diğer faaliyetlerinin belirlenmiş yordamlara, politikalara, kurallara ve kanuni mevzuata uygun olup olmadığını tespit etmek amacıyla incelenmesidir. Bu denetim türünde önceden belirlenmiş ölçütler, hem işletme yönetiminden hem de yasalar ve diğer devlet düzenlemelerinden kaynaklanabilir.

***Performans Denetimi***; işletmenin ya da işletmenin bir bölümünün görev ve sorumluluklarını yerine getirirken kullandığı fiziki, mali ve beşeri kaynakların etkinlik ve verimlilik derecelerinin değerlendirilmesidir. Etkinliğin ve verimliliğin ölçütlerini değerleme konusunda karşılaşılabilen zorluklar nedeniyle, diğer denetim türlerine göre nispeten daha güç bir denetimdir. Bu nedenle kıdemli denetçiler tarafından yapılması daha doğrudur.

***Bilgi Teknolojileri Denetimi***; denetlenen birimin elektronik bilgi sistemlerinin sürekliliğinin ve güvenilirliğinin değerlendirilmesidir. Ayrıca bu denetim türü, denetlenen bilgi sisteminde depolanan veri ve bilgilerin yeterliliğini ve doğruluğunu değerlendirmek için kullanılır. Bilgi sistemine yetkisiz erişimin engellenmesi, bilgi sisteminin yazılım ve donanımının korunması ve bilgi sisteminde yapılan hatalı ve hileli işlemlerin önlenmesi gibi kontrollerin değerlendirilmesini kapsar.

***Sistem Denetimi***; denetlenen birimin faaliyetlerinin, yönetim veya iç kontrol sisteminin; örgütsel yapısına katkı sağlayıcı bir yaklaşımla analiz edilmesi, eksikliklerinin tespit edilmesi, kalite ve uygunluğunun araştırılması, kaynakların ve uygulanan yöntemlerin yeterliliğinin ölçülmesi suretiyle değerlendirilmesidir.

İç denetim değerlendireceği yönetim ve kontrol faaliyetinin içerisinde yer almamalıdır. Ancak iç denetimden hazırlanan bir faaliyet ya da programa ilişkin sistem ve yordamlar temelinde bir ön değerlendirme yapması ya da fikir beyan etmesi beklenir. İç denetim asla devamlı surette iç kontrol faaliyetinin bir parçası haline gelmemelidir. Böylece iç denetimin, yönetimin üzerinde olması gereken iç kontrol sorumluluğunu asla paylaşmadığı kesin bir biçimde ortaya konmuş olur (Alptürk, 2008, s.23).

## 2.11. Uluslararası İç Denetçiler Enstitüsü ve Mesleki Uygulama Çerçevesi

1941 yılında kurulan Uluslararası İç Denetçiler Enstitüsü (IIA) genel merkezi Amerika'nın Florida eyaletinin Altamonte Springs şehrinde bulunan uluslararası bir meslek örgütüdür. IIA'nın iç denetim, risk yönetimi, yönetişim, iç kontrol, bilgi teknolojileri denetimi, eğitim ve güvenlik alanlarında uzmanlaşmış 116 ülkeden 180.000'den fazla üyesi bulunmaktadır. IIA, iç denetçilik mesleğinin dünya genelinde kabul edilmiş otoritesidir. İç denetim mesleğinin etkisinin giderek artmasında önemli bir rol oynamaktadır. İç denetimin mesleki rehberi olarak, etik ilkeler ve uygulama standartları oluşturur. Üyelerini mesleki anlamda destekler ve eğitim programları hazırlar. Mesleğin baş eğitimcisi olarak yeterlik sınavını geçen meslek mensuplarının sertifikasyon hizmetini sağlar.[1]

IIA, iç denetimin dünya çapında uygulanmasına rehberlik etmek amacıyla standartlar ve uygulama rehberleri hazırlar. IIA, mesleki rehberliğini Uluslararası Mesleki Uygulama Çerçevesini (International Professional Practices Framework) hazırlayarak yapar. Çerçeve, zorunlu rehber ve kuvvetle tavsiye edilen rehberden oluşur. Zorunlu rehber; iç denetim tanımı, iç denetimin mesleki uygulamaları için çekirdek ilkeler, etik ilkeler ve Uluslararası İç Denetim Mesleki Uygulama Standartlarından oluşur. Kuvvetle tavsiye edilen rehber ise; pozisyon raporları, uygulama önerileri ve uygulama rehberlerinden oluşur (Johnstone vd., 2014, s.762).

### 2.11.1. İç denetimin mesleki uygulamaları için çekirdek ilkeler

Bir bütün olarak ele alındığında çekirdek ilkeler, iç denetimin etkinliğini açıkça ortaya koyar. İç denetim biriminin etkinliği için bütün ilkelerin eksiksiz bir şekilde uygulanması gerekir. Çekirdek ilkeler ile iç denetimin etkinliğinin temel özellikleri şöyle sıralanmıştır (Messier vd., 2016, s.728):

- Dürüst ve faziletli davranır.
- Yetkinlik ve mesleki özen sergiler.
- Objektiftir ve asla etki altında kalmaz (bağımsızdır).
- Kurumun stratejileri, hedefleri ve riskleri ile uyumludur.
- İşletme içinde uygun olarak konumlandırılmıştır ve yeterli kaynağa sahiptir.
- Kalite ve sürekli gelişimi esas alır.

[1] Ayrıntılı bilgi için bakınız: https://www.theiia.org/

- Etkili bir şekilde iletişim kurar.
- Risk odaklı güvence sağlar.
- Öngörülü, proaktif ve gelecek odaklıdır.
- Kurumsal gelişimi teşvik eder.

### 2.11.2. Etik ilkeler

IIA'nın uygulama çerçevesinde zorunlu rehberin bir parçası olan etik ilkeler, iç denetim mesleğinde etik kültürü desteklemek için geliştirilmiştir. Etik ilkeler, iç denetçilerin uygulaması gereken ahlaki sorumluluklardır. Etik ilkeler, dört temel ilkeden oluşur;

- ***Dürüstlük***: İç denetçilerin dürüstlüğü güven sağlar ve böylece denetim yargılarına ilişkin bir güven temeli oluşturur.
- ***Objektiflik***: İç denetçiler inceledikleri faaliyet veya süreç hakkında bilgiyi toplarken, değerlendirirken ve raporlarken en yüksek seviyede mesleki objektiflik sergilerler. İç denetçiler, tüm ilgili şartları dengeli bir şekilde değerlendirirler ve denetim yargılarını oluştururken kendilerinin veya başkalarının menfaatlerinden asla haksız yere etkilenmezler.
- ***Gizlilik***: İç denetçiler aldıkları bilginin değerine ve sahipliğine saygı gösterirler ve yasal ya da mesleki bir zorunluluk bunu gerektirmedikçe, gerekli yetkilendirme olmadan bilgiyi açıklamazlar.
- ***Yetkinlik***: İç denetçiler, iç denetim hizmetinin sunulması için gerekli olan bilgi, yetenek ve tecrübeyle hareket ederler.

IIA tarafından, Etik İlkelerin uygulanmasını kolaylaştırmak, iç denetçiler tarafından yorumlanmasına yardımcı olmak ve nasıl davranmaları gerektiği konusunda rehberlik etmek amacıyla, iç denetçilerden beklenen davranışları tanımlayan Davranış Kuralları geliştirilmiştir. IIA'nın davranış kuralları Tablo 2.2'de sunulmuştur.

**Tablo 2.2.** *IIA Davranış Kuralları (https://www.tide.org.tr/page.aspx?nm=etik_kurallar)*

| Etik İlkeler | Beklentiler |
|---|---|
| ***Dürüstlük*** | İç denetçiler;<br>1.1. Çalışmalarını doğruluk, dikkat ve sorumluluk duygusuyla yürütmelidirler.<br>1.2. Hukuka uygun hareket ederler, yasaların ve mesleğin gerektirdiği açıklamaları yaparlar.<br>1.3. Herhangi bir yasadışı faaliyetin bilerek veya isteyerek bir parçası olmazlar ve iç denetim mesleğine ya da işletmeye karşı yüz kızartıcı bir eylemde bulunmamalıdırlar.<br>1.4. İşletmenin meşru ve ahlaka uygun amaçlarına saygı duymalı ve katkı sağlamalıdırlar. |
| ***Objektiflik*** | İç denetçiler;<br>2.1. Değerlendirmelerinin tarafsızlığına gölge düşürebilecek veya potansiyel olarak zarar verebilecek herhangi bir ilişkiye veya faaliyete, kendi işletmelerinin çıkarlarıyla çatışsalar bile katılmamalıdırlar.<br>2.2. Mesleki yargılarını zayıflatabilecek veya zayıflatacağı varsayılan herhangi bir şeyi kabul etmemelidirler.<br>2.3. Tespit ettikleri ve açıklanmadığında inceledikleri faaliyetlerin raporlanmasına zarar verebilecek tüm önemli bulguları açıklamalıdırlar. |
| ***Gizlilik*** | İç denetçiler;<br>3.1. Görevleri sırasında elde ettikleri bilgilerin kullanımı ve korunması konusunda tedbirli davranmalıdırlar.<br>3.2. Elde ettikleri bilgileri kişisel bir amaçla, illegal olarak ve işletmenin meşru ve ahlaka uygun amaçlarına zarar verecek şekilde kullanmamalıdırlar. |
| ***Yetkinlik*** | İç denetçiler;<br>4.1. Sadece görevin gerektirdiği bilgi, beceri ve tecrübeye sahip oldukları işleri üstlenmelidirler.<br>4.2. İç denetim hizmetlerini, Uluslararası İç Denetim Meslekî Uygulama Standartlarına uygun bir şekilde yerine getirmelidirler.<br>4.3. Sürekli olarak kendi yeterliklerini ve hizmetlerinin kalitesini geliştirmelidirler. |

### 2.11.3. Uluslararası iç denetim mesleki uygulama standartları

IIA tarafından hazırlanan standartlar, iç denetim alanında hazırlanan uluslararası kabul görmüş tek standartlar setidir. IIA standartları, iç denetçilere faaliyetlerinde rehberlik etmek üzere tasarlanmıştır. İç denetçilerin görevlerini yaygın olarak kabul edilmiş uygulamaları kullanarak, ahlaka uygun bir şekilde ve sorumluluklarını bilerek yerine getirmelerini sağlar. Standartların uygulanması yönetime ve denetim komitesi gibi diğer paydaşlara, iç denetim biriminin faaliyetlerini profesyonel bir biçimde yürüttüğüne dair güvence verir. İşletme yönetiminin iç denetim biriminin faaliyetlerini mesleki normlarla karşılaştırabilmesine olanak tanır ve iç denetimin kalitesinin artırılmasını sağlar. Standartlar, ilkesel tabanlı olarak hazırlanmıştır; emredici ve uygunsuz kısıtlayıcı hükümler içermez. İç denetçilere faaliyetlerine yönelik ölçütler sağlar ve onların yenilikçi ve yaratıcı olmalarına engel olmaz. (Pitt, 2014, s.11).

Standartların amaçları IIA Uluslararası Mesleki Uygulama Çerçevesinde şöyle sıralanmıştır (IIA, 2010a, s.3-4):

- İç denetim uygulamasını olması gerektiği gibi temsil eden temel ilkeleri tanımlamak.
- Katma değerli iç denetim faaliyetlerini teşvik etmeye ve hayata geçirmeye yönelik bir çerçeve oluşturmak.
- İç denetim performansının değerlendirilmesine uygun bir zemin oluşturmak.
- Gelişmiş kurumsal süreç ve faaliyetleri canlandırmak.

Standartlar; nitelik standartları ve performans standartları olarak ikiye ayrılır. Nitelik standartları, iç denetim biriminin ve iç denetçilerin taşıması gereken özellikleri tanımlarken; performans standartları, iç denetim faaliyetlerinin yürütülmesi, sonuçların izlenmesi ve raporlanmasında iç denetçilere yol gösterir ve iç denetim faaliyetinin kalitesini belirleyen performans değerlendirme ölçütlerini ortaya koyar.

İç denetim faaliyetinin kalitesi açısından standartlara uyum büyük önem taşır. İşletme içinde, iç denetim faaliyetinin amaç, yetki ve sorumlulukları standartlarla uyumlu bir yönetmelikle açıkça tanımlanmalıdır. İç denetçiler, standartlara uyum sağlayamadıkları durumlar için özel durum açıklamalarında bulunmalıdırlar. Ayrıca iç denetim standardı 1312'ye göre; iç denetim biriminin en azından beş yılda bir kez, standartlara uyum göstermeyi de kapsayacak şekilde, işletme dışından bir gözden geçirme uzmanı ya da ekibi tarafından yapılması gereken bir bağımsız kalite değerlendirmesinden geçmesi gerekir.

IIA İç Denetim Standartları Kurulu, iç denetimin değişen koşullara ve ortaya çıkan ihtiyaçlara cevap verebilmesi amacıyla gerekli gördüğünde standartlarda değişiklikler yapmaktadır. Kurul standartlarla ilgili olarak tavsiye ve değerlendirmelerin kendisine iletilmesini istemektedir. Ayrıca değişiklikleri onaylamadan önce taslak metni, tartışılmak ve değerlendirilmek üzere kamuoyuna sunar. Bu süreç, standartların geliştirilmesinde önemli bir adım olarak görülür. IIA, 1 Ocak 2013 tarihinde standartların gözden geçirilmiş son halini yayımlamıştır. İç denetim standartları Tablo 2.3'te özetlenmiştir.

**Tablo 2.3.** *Uluslararası İç Denetim Standartları (IIA, 2010a)*

| Standart | Tanım |
|---|---|
| ***Nitelik Standartları*** | |
| 1000- Amaç, Yetki ve Sorumluluklar | "İç denetim faaliyetinin amaç, yetki ve sorumlulukları, Standartlarla uyumlu olan ve denetim komitesi ile yönetim kurulunca da onaylanan bir yönetmelikte açıkça tanımlanmalıdır. |
| 1100- Bağımsızlık ve Objektiflik | İç denetim faaliyeti bağımsız olmalı ve iç denetçiler görevlerini yaparken objektif davranmalıdır. |
| 1200- Yeterlilik ve Azamî Mesleki Özen ve Dikkat | Görevlendirmeler, yeterlilik ve azamî meslekî özen ve dikkat ile yerine getirilmelidir. |
| 1300- Kalite Güvence ve Geliştirme Programı | İç denetim yöneticisi, iç denetim faaliyetinin tüm yönlerini kapsayan ve etkinliğini sürekli gözleyen bir kalite güvencesi ve geliştirme programı hazırlamalı ve bunu sürdürmelidir. |
| ***Performans Standartları*** | |
| 2000- İç Denetim Faaliyetinin Yönetimi | İç Denetim Yöneticisi, iç denetim faaliyetini, faaliyetin kuruma değer katmasını sağlayacak etkili bir tarzda yönetmelidir. |
| 2100- İşin Niteliği | İç denetim faaliyeti; sistematik ve disiplinli bir yaklaşımla, risk yönetimi, kontrol ve yönetişim sistemlerini değerlendirmeli ve bu sistemlerin iyileştirilmesine katkıda bulunmalıdır. |
| 2200- Görev Planlaması | İç denetçiler, her görev için, kapsam, amaçlar, zamanlama ve kaynak dağılımı hususlarını da dikkate alan ayrı bir plan hazırlamalı ve kaydetmelidir. |
| 2300- Görevin Yapılması | İç denetçiler, üstlendikleri görevin hedeflerine ulaşmak için yeterli bilgileri belirlemeli, analiz etmeli, değerlendirmeli ve kaydetmelidir. |
| 2400- Sonuçların Raporlanması | İç denetçilerin, denetim sonuçlarını raporlaması gerekir. |
| 2500- İlerlemenin Gözlenmesi | İç Denetim Yöneticisi, yönetime rapor edilen sonuçların akıbetinin gözlenmesi için bir sistem kurmalı ve uygulamalıdır. |
| 2600- Yönetimin Artık (Bakiye) Riskleri Üstlenmesi | İç Denetim Yöneticisi, üst yönetimin kurum için kabul edilemeyecek bir artık (bakiye) risk düzeyini üstlenmeyi kabul ettiğine inandığı takdirde, konuyu üst yönetimle tartışmalıdır." |

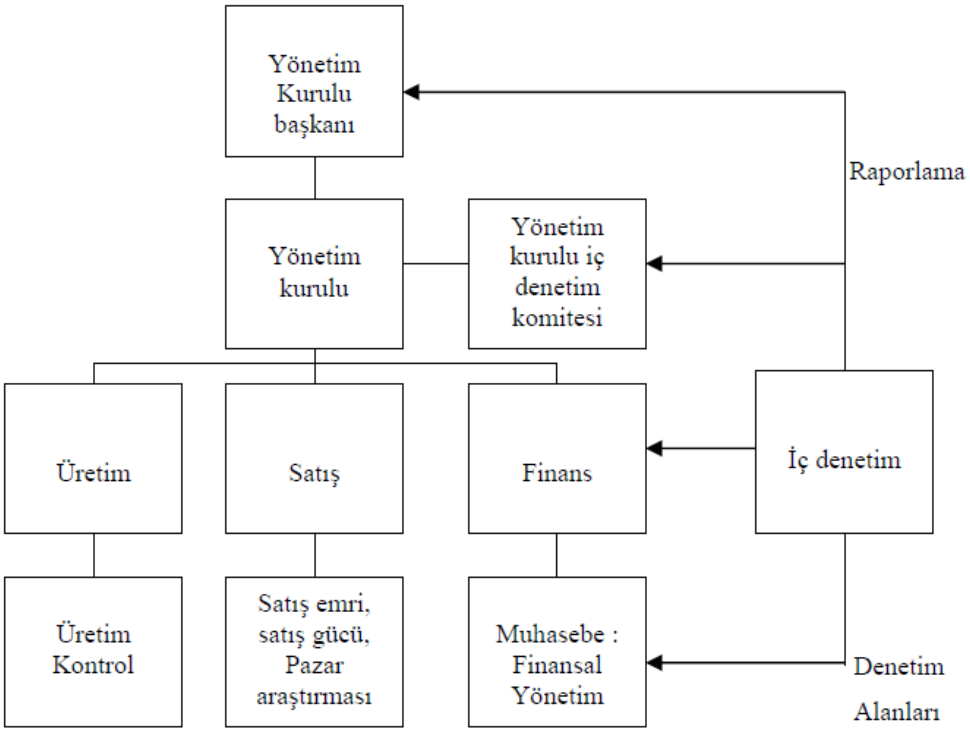
## 2.12. İç Denetimin İşletme Organizasyonundaki Yeri

Bir işletmede iç denetim faaliyetinin etkili ve rasyonel kullanılabilmesi amacıyla, iç denetim hizmetinin işletmeye sunulması için üç temel yaklaşımdan biri tercih edilebilir. Bu yaklaşımlar (Uzun, 2012, s.85-86);

- ***İç kaynak kullanımı***: İşletme içinde iç denetim birimi kurularak veya iç denetçi istihdam edilerek iç denetim faaliyetinin yürütülmesidir. BDDK'nın getirdiği düzenlemelere göre bankalarda iç denetim birimi kurulması bir zorunluluktur.
- ***Dış kaynak kullanımı***: Bir denetim firmasından iç denetim hizmetinin satın alınmasıdır.
- ***Eş kaynak kullanımı***: İç denetim faaliyetinin yürütülmesi için, hem işletme içinde istihdam edilmiş iç denetçilerden hem de bir denetim firmasının denetçilerinden yararlanılmasıdır.

İç denetim faaliyeti söz konusu yaklaşımlardan anlaşılacağı üzere, sadece işletme içinde bir iç denetim birimi kurularak ya da işletmeye iç denetçiler alınarak yürütülebilen bir faaliyet olmayıp, profesyonel bir firmadan iç denetim hizmeti satın alınarak da yürütülebilir. Hangi yaklaşımın işletme için uygun olduğu işletmenin büyüklüğüne, işletmenin faaliyet gösterdiği endüstride konuya ilişkin düzenlemelerin öngördüğü esaslara ve yönetimin iç denetime yönelik tutum ve anlayışına göre değişir. İşletme yönetiminin işletmeye en uygun yaklaşımı belirlemesi ve etkin iç denetim için gereken yönetsel desteği vermesi büyük önem taşır (Uzun, 2012, s.86).

Büyük işletmelerde iç denetim fonksiyonu geniş biçimde örgütlenmiş bir birim olarak yer alabilir ve çok önemli görevler üstlenir. Bu birim yönetim kuruluna bağlı olarak faaliyet gösterir. İç denetim, yönetim adına denetim yapar. Yönetim tarafından konulmuş ölçütlere uyulup uyulmadığı ve işletme politika ve yordamlarının işlevselliğini araştırmak ve gerektiğinde yeni yordamlar tasarlamak iç denetimin öncelikli sorumluluklarındandır. İç denetimden yönetime gelecek raporlar, yönetimin özellikle iç kontrol hakkındaki kararlarını etkileyecektir. Örneğin, iç denetim, kullanılmakta olan bilgisayar sisteminin donanım veya yazılımının iç kontrolün etkinliği konusunda yetersiz kaldığını saptayarak, bunu üst yönetime raporlayabilir. Böyle bir rapor, üst yönetimin, ihtiyaçlara uygun yeni bir bilgisayar sistemi için yatırım kararı almasını sağlayabilir (Erdoğan, 2005, s.6-7). İç denetim biriminin işletme organizasyonu içerisindeki konumu Şekil 2.5'te gösterilmiştir.




**Şekil 2.5.** *İç Denetimin İşletme Organizasyonunda Yeri (Erdoğan, 2005)*

İç denetim biriminin örgütsel statüsü, iç denetçilerin yetki ve sorumluluklarına göre hareket edebilmelerini sağlayacak biçimde olmalıdır. Örgütsel statü, iç denetim biriminin örgütsel hiyerarşideki yeridir. İç denetçiler, denetledikleri birimlerle işbirliği yapabilmek ve çalışmalarının bağımsızlığını ve objektifliğini koruyabilmek için yönetimin desteğine ihtiyaç duyarlar. Üst yönetim tarafından iç denetçilerin görev, yetki ve sorumlulukları yönetmelik, genelge ya da benzer bir yazılı belgeyle tanımlanmalıdır. Üst yönetimin hazırladığı bu belge, iç denetim biriminin örgüt içindeki konumunu belirlemeli, iç denetçiye denetim işinin yürütülmesine ilişkin kayıt, personel ve fiziki varlıkları inceleme yetkisini verdiğini açıkça belirtmeli ve iç denetim faaliyetinin kapsamını tanımlamalıdır. İşletme içinde üst yönetim tarafından iyi hazırlanmış böyle bir belgenin varlığı, iç denetim biriminin etkin ve düzenli bir şekilde çalışmasını sağlar. İşletme yönetimi, iç denetim politikasını yazılı bir belgeyle ortaya koymazsa, iç denetim faaliyetinin etkin ve verimli bir şekilde yürütülmesi mümkün olmaz (Kepekçi, 1982, s.42-43).

Çağdaş işletme yönetiminde, örgütsel yapıdaki farklı hiyerarşik basamaklar ve biçimsel ilişkiler sonucu ortaya çıkan yetki türleri içinde, iç denetim biriminin örgütsel statüsüne göre, sahip olması gereken yetki türü kurmay yetkisidir. Kurmay yetkisi işletme içinde bu yetkiye sahip olan birime veya kişiye danışmanlık yapma hakkı verir. Öte

yandan kurmay birimlerin yöneticileri kendi birimleri dışında emir verme ve iş yaptırma yetkisine sahip değillerdir. Bu yetkiye sahip kişiler, kendi uzmanlık alanlarıyla ilgili konularda, yöneticilere bilgi aktararak alınacak kararların daha isabetli olmasını sağlarlar. Organizasyonlar büyüdükçe, bu yetkiye duyulan ihtiyaç artar (Boone & Kurtz, 2013, s.241-242; Şakar, 2013, s.75).

Bir işletmede hem muhasebe hem de yönetsel iç kontrollerin kurulmasında ve işletilmesinde temel sorumluluk işletmenin üst yönetiminindir. İç denetim işletme içinde bağımsız olarak kurulan ve işletme faaliyetlerini bağımsızca inceleyen, analiz eden ve değerleyen bir işlevdir. Yönetimin amaçlarına ulaşması konusunda makul güvence sağlamak amacıyla faydalanılan bir yönetim aracıdır. İç denetim yapısının yeterliliği ve etkinliğinden de üst yönetim sorumludur. İç denetçiler, danışmanlık hizmeti sunarken bağımsızlıklarını muhafaza etmeli ve asla idari sorumluluk üstlenmemelidir (Uzun, 2012, s.80-81).

### 2.13. İç Denetçilerin Özellikleri

Yoğun rekabetin yaşandığı ve risklerle örülü günümüzün işletme ikliminde kontrollerin izlenmesi, operasyonel etkinliğin değerlendirilmesi ve yönetimin stratejilerinin ve her türlü girişiminin desteklenmesi gibi faaliyetleriyle iç denetim fonksiyonunun, yönetişimi geliştiren ve anahtar yönetişim süreçlerini destekleyen en nitelikli meslek grubu olarak görülmesi tesadüf değildir. Bununla birlikte hizmet talebindeki bu muazzam artıştan yararlanmak için iç denetçilerin beceri, nitelik ve yetkinliklerini oldukça geliştirmeleri, işletmelerindeki örgütsel durumlarını ve konumlarını yükseltmeleri ve kendilerini bunlara uygun bir şekilde değiştirmeleri gerekmektedir (Ramamoorti, 2003, s.9).

Günümüzde işletmelerin önemli risk yönetimi sorunlarını gidermeye çalışırken iç denetim birimlerinin daha fazla liderlik rolünü üstlenmesi bir ihtiyaçtır – ve bir fırsattır. İşletmedeki konumunu yükseltmek için, iç denetimin üç ana hedef üzerinde yoğunlaşması gerekir (Schweik & Watts, 2015, s. 2):

- İşletmelerin önemli risklerini denetlemek için teknik becerileri edinin. Uygun deneyime sahip denetçiler işe alınabilir, işletme içinde uygun görülen denetçilere eğitim verilebilir veya her ikisi birden uygulanabilir.

- İşletmenin sektörünü ve karşılaştığı riskleri tam olarak anlayın. Öncelikli piyasa yönlendiricilerinin ve yürürlükte olan yasal düzenlemelerin bilgisi elde edilmelidir. Rekabet şartları anlaşılmalıdır.
- İç denetim becerilerini ve bilgisini daha etkili hale getirebilecek teknoloji ve yazılım araçlarını kullanın.

21. yüzyılın iç denetçileri, faaliyetler (kontrol sistemleri dahil), performans, bilgi ve bilgi sistemleri, yasal ve yasal olmayan uygunluk, mali tablolar, çevresel raporlama ve çevresel performans, hile ve kalite dahil neredeyse işletmeye dair her şeyi denetlemek için hazır olmalıdırlar. Denetçiler aşağıdaki alanlarda uzmanlaşmalıdır (Ratliff & Reding, 2002, s. 11):

- Analitik ve eleştirel düşünce becerisi,
- Denetlenen herhangi bir kişi, işletme veya sistemin yeterince anlaşılmasını sağlayan etkili bir metodoloji,
- İç kontrole ilişkin yeni kavramlar, teknikler ve ilkeler,
- Hem denetlenen hem de denetçiyle ilişkili risk ve fırsatların farkında olunması ve anlaşılması,
- Her bir denetim projesi için genel ve özel denetim amaçlarının geliştirilmesi,
- Denetim kanıtlarını seçme, toplama (geniş bir denetim yordamları seti kullanarak), değerlendirme ve istatistiksel-istatistiksel olmayan teknikler dâhil olmak üzere belgelendirme,
- Denetim sonuçlarını çeşitli alıcılara çeşitli formatlarda raporlama,
- Mesleki etik,
- Çeşitli denetim raporu türleri için uygulanabilir denetim teknolojisi.

Benzer şekilde, Moeller & Witt (1999, s. 14-15) başarılı bir iç denetçi olmak için gerekli kişisel nitelikleri şöyle sıralamıştır (teknik ve mesleki niteliklere ek özellikler barındıran bir listedir): (1) Temel adalet ve dürüstlük; (2) işletmenin menfaatlerine olan bağlılık; (3) makul seviyede alçak gönüllülük; (4) mesleki zekâ; (5) empati; (6) rolü ve konumuyla tutarlılık; (7) merak; (8) eleştirel tutum; (9) uyanıklık; (10) sabır; (11) enerji; (12) kendine güven; (13) cesaret; ve (14) güçlü kararlar verme becerisi.

## 2.14. İç Denetim ve Bağımsız Denetim İlişkisi

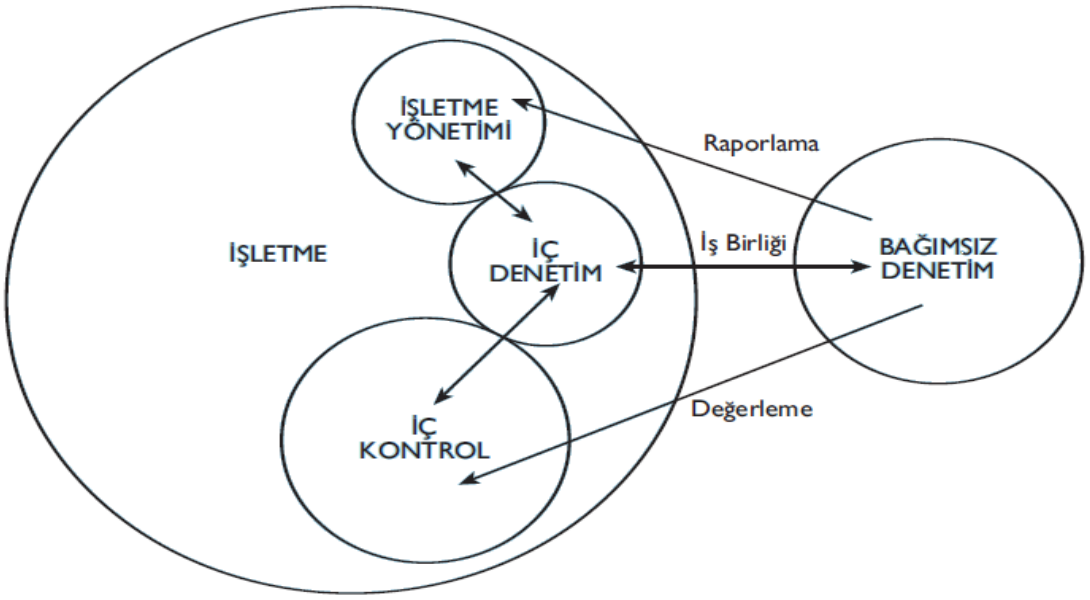
İç denetçi ve bağımsız denetçi tarafından yürütülen işin türü ve amaçları birbirinden oldukça farklıdır. Ancak düşünüldüğünde aralarında önemli bir örtüşme olduğu anlaşılır. Bağımsız denetçiler, işletmenin finansal tablolarının önemli yanlışlıklar içerip içermediği hakkında görüş oluşturmayı amaçlarlar. Bağımsız denetçiler, önemlilik kavramına bağlı olarak hareket ettikleri için, genellikle belirli bir alandaki denetimlerle yoğun bir şekilde ilgilenmezler. Finansal tabloların tamamında önemli yanlışlıklar olmadığına dair makul güvence elde edinceye kadar kanıt toplarlar. Daha sonra raporlarını, denetledikleri işletmenin dışındaki taraflara sunarlar. Diğer taraftan iç denetçiler, yasalara ve düzenlemelere uygunluğu ve operasyonel verimliliği değerlendirerek, işletmenin maruz kaldığı riskleri yöneterek ve özel dikkat gerektiren alanlarda detaylı finansal denetimler yaparak işletme yönetimine ve yönetim kuruluna yardım ederler (Messier vd., 2016, s.732-733).

İki disiplin arasında iç kontrolü değerleme, faaliyet denetimi ve özel amaçlı denetim çalışmalarında uyguladıkları yöntemler ve denetim testleri bakımından farklılık yoktur. Ancak bağımsız denetçilerin asıl ilgilendikleri, finansal tabloları etkileyen önemli olaylarken, modern iç denetçiler bütün örgütü etkileyen olayları test eder ve değerlerler. Yönetim perspektifi açısından karşılaştırdığımız zaman, iç denetçilerin faaliyetleri daha kapsamlı ve ayrıntılıdır (Sawyer, 1993, s.45). İç denetim ve bağımsız denetim arasındaki temel farklar Tablo 2.4'te gösterilmiştir.

**Tablo 2.4.** *İç Denetim ve Bağımsız Denetim Arasındaki Farklılıklar (Sawyer, Dittenhofer, Scheiner, 2005, s. 7-8)*

| İç Denetçi | Bağımsız Denetçi |
|---|---|
| İşletmenin bir çalışanıdır. | Bağımsız bir taraftır. |
| İşletmeye hizmet eder. | Güvenilir finansal bilgiye ihtiyaç duyan üçüncü taraflara hizmet eder. |
| Gelecek odaklıdır. İşletmenin amaçlarına ulaşmasını sağlamak için tasarlanmış olan kontrolleri değerlendirir. | Finansal tablolarda yer alan geçmişteki olayların doğruluğu ve anlaşılabilirliğine odaklanır. |
| İncelediği her faaliyette direkt olarak herhangi bir şekil veya ölçüdeki hilenin önlenmesiyle ilgilenir. | Hilenin bulunması ve önlenmesiyle finansal tabloların önemlilik düzeyini maddi olarak etkileme ihtimali olursa direkt olarak ilgilenir. Onun dışında direkt ilgilenmez. |
| Denetim faaliyetlerinde bağımsızdır, fakat yönetimin bütün bileşenlerinin isteklerine ve ihtiyaçlarına cevap vermeye hazırdır. | Hem şeklen hem de mental tavır anlamında yönetimden ve yönetim kurulundan bağımsızdır. |
| Faaliyetlerini sürekli olarak devam ettirir. | Finansal tabloları destekleyen kayıtları periyodik olarak, genellikle yılda bir kez inceler. |

İç denetçiler ve bağımsız denetçiler faaliyetlerinde koordinasyon içinde olmalıdırlar. İç denetçilerin ve bağımsız denetçilerin amaçları ve elde etmek istedikleri sonuçlar farklı olsa da, finansal tabloların denetiminde kullandıkları teknikler benzerdir. İki farklı meslek birbirlerine saygı duymalı ve birbirlerinin yeteneklerinden faydalanmalıdırlar (Sawyer vd., 2005, s.8). Bağımsız denetçiler aralarında koordinasyon ve işbirliğini geliştirerek, finansal tabloları daha etkin ve verimli bir şekilde denetleyebilirken; iç denetçiler de iç kontrole değer katmak için bağımsız denetçilerin çalışmalarından faydalanabilirler (Wood, 2004: 2). Şekil 2.6'da, bağımsız denetim ve iç denetim ilişkisi, işletme yönetimiyle ilişkiler ve iç kontrolün değerlendirilmesi bağlamında gösterilmiştir.




**Şekil 2.6.** *Bağımsız Denetim – İç Denetim İlişkisi (Erdoğan, 2012, s. 96)*

Bağımsız denetçiler, denetim risk modelini kullanırken, kontrol riskini değerlendirmek için iç denetçilere güvenebilirler. Eğer etkin bir iç denetim varsa, bağımsız denetçiler kontrol riskini önemli ölçüde düşük belirleyebilirler ve bunun sonucunda da tözel testlerin kapsamı daralır. Sonuç olarak, bağımsız denetçiler müşterileri iyi işleyen bir iç denetim sistemine sahip olduklarında denetim ücretlerini önemli tutarda azaltabilirler. Bağımsız denetçiler, iç denetçilerin etkinliğini genellikle aşağıda yer alan ölçütlere göre değerlendirirler (Arens vd., 2012, s.818);

- İç denetim biriminin bağımsızlığı,

- Mesleki uzmanlığı ve eğitimi,
- Finansal tablolara ve iç kontrole ilişkin denetim testlerindeki performans.

Denetim standartları bağımsız denetçinin, iç denetçinin doğrudan yardımını denetiminde kullanmasına izin verir. Bağımsız denetçi, iç denetim personelinin denetim testlerindeki performansına güvenerek, denetimini daha kısa zamanda ve daha az maliyetle tamamlayabilir. İç denetçiler, bağımsız denetçiye doğrudan yardım sağladıkları zaman, bağımsız denetçi, onların yetkinliğini, bağımsızlığını ve yaptıkları işin kalitesini değerlendirmelidir (Arens vd., 2012, s.818).

AICPA tarafından yayımlanan 65 numaralı standarda göre, bağımsız denetçi ve iç denetçi arasında etkin bir koordinasyon ve işbirliğini sağlamak amacıyla yapılması gereken başlıca faaliyetler şöyle sıralanmıştır (SAS No:65):

- "Periyodik olarak belirli dönemlerde toplantılar yapmak,
- Potansiyel muhasebe ve denetim problemlerini tartışmak,
- Birbirlerinin denetim programlarına ve çalışma kâğıtlarına erişim,
- Denetim raporlarının incelenmesi,
- Denetim kavramlarıyla ilgili ortak bir terminoloji oluşturmak."

Bağımsız denetçi – iç denetçi ilişkisini düzenleyen ve denetçilere rehberlik eden standartlar şunlardır:

- Amerikan Sertifikalı Muhasebeciler Enstitüsü (American Institute of Chartered Public Accountant - AICPA) tarafından yayımlanan Denetim Standardı 65 (Statement on Auditing Standart – SAS 65) iç denetçinin çalışmalarının ve iç denetçinin doğrudan yardımının kullanımının değerlendirilmesinde bağımsız denetçiye rehberlik eder.
- Uluslararası Muhasebeciler Federasyonu (The International Federation of Accountants - IFAC) tarafından yayımlanan Uluslararası Denetim Standardı 610, (International Standard on Auditing – ISA 610) bağımsız denetçinin uygulayacağı denetim yordamlarının niteliğini veya zamanlamasını değiştirmek veya kapsamını daraltmak amacıyla, işletmenin iç denetim fonksiyonunun çalışmasını kullanmayı planladığı durumlarda denetçilere rehberlik eder.
- İç Denetçiler Enstitüsü (The Institute of Internal Auditors – IIA) tarafından Uluslararası İç Denetim Mesleki Uygulama Standardı 2050-1 Eşgüdüm ve 2010-2 Bağımsız Denetim Hizmetlerinin Satın alınması (The International Standards for the Professional Practice of Internal Auditing) yayımlanmıştır. Bu standartlara

göre, iç denetim yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer iç ve dış sağlayıcılarla, mevcut bilgileri paylaşmalı ve faaliyetleri bunlarla eşgüdüm içinde sürdürmelidir. Ayrıca standartlar, iç denetçilerin kurum için bağımsız denetçilerin seçilmesi sürecine katılımını düzenler.

Bağımsız denetçiler ve iç denetçiler arasında koordinasyonun ve işbirliğinin geliştirilmesi, hem denetçilerin çalışmalarına hem de hizmet sunulan işletmeye çeşitli faydalar sağlar. Bu faydalar şöyle sıralanabilir:

- Bağımsız denetçiler çok sayıda işletmeye hizmet verdikleri için, iç denetçilere kıyasla çok daha fazla farklı durumla karşılaşmakta ve sorunlara farklı çözümler getirebilmektedirler. İç denetçiler, bağımsız denetçilerin yaptıkları diğer denetimlerden elde ettikleri mesleki tecrübeyle işletmenin iç kontrolleriyle ilgili incelemelerinden ve değerlendirmelerinden faydalanma imkânı elde ederler (Tuan, 2015, s.324).
- İç denetçiler, denetlenen işletmenin bir çalışanı olduklarından işletmenin faaliyetleri ve örgüt kültürü hakkında daha fazla bilgiye sahiplerdir. Bağımsız denetçiler, iç denetçilerin çalışmalarından ve bilgilerinden faydalanarak, uygulayacakları denetim yordamlarını daha kolay saptarlar ve iç kontrol hakkında daha kolay bilgi edinirler.
- Bağımsız denetçiler, iç denetçilerin bağımsız denetimin amaçlarını ve standartlarını anlamalarına yardımcı olur. Yeni ve farklı denetim yordamları ve bilgi alış verişiyle iç denetim çalışanlarının bilgi düzeyi artar. Bağımsız denetçilerin, iç denetim programları ve içeriği hakkında yaptıkları eleştiriler ve bağımsız denetim sürecinde örgüt içinde daha önce fark edilmemiş olan riskli alanların keşfedilmesi, iç denetimin kalitesini artırır (Uzay, 1999, s.68).
- İç denetçilerin çalışmalarından faydalanarak bağımsız denetçiler, işletmenin finansal olmayan yönünün, finansal tabloları nasıl etkilediğini daha net tespit edebilirler.
- Bağımsız denetçiler, iç denetçilerin çalışmalarını izlerken, gözlem konusunda tecrübe kazanır ve bunu kendi elemanlarını izlerken kullanabilir.

- İç denetim çalışanları, bağımsız denetçilerle koordinasyon ve işbirliği halinde yürütülen bir denetim süreci sayesinde işbirliği halinde çalışma disiplini kazanabilirler.
- İç denetçilerin hazırladığı yönetim raporları ve çalışma kâğıtları, bağımsız denetçiler için iç kontrolün niteliği hakkında bir kanıt kaynağı ve iç kontrolü incelemek için hazırlayacağı belgeler için kılavuz niteliğindedir (Uzay, 1999, s.68).
- İyi koordine edilmiş bir denetim süreci ve etkin işbirliği, tekrarlanan çalışmalar için harcanan emeği azaltarak zaman ve kaynak tasarrufu sağlar. Böylece denetçiler, diğer sorumlulukları üzerine daha fazla odaklanma imkânı elde ederler (Fowzia, 2010, s.28).
- Bağımsız denetçinin ve iç denetçinin denetim sürecinde işbirliği yapması, tekrarlanan çalışmaları ortadan kaldırarak, harcanan zaman ve çabayı dolayısıyla da denetim maliyetlerini azaltır. Bağımsız denetçiler, işbirliğinden elde edeceği maliyet tasarrufu ile iç denetçilerin çalışmalarına güvenmenin sonucunda ortaya çıkan riskleri iyi değerlendirmelidir (Suwaidan & Qasim, 2010, s.509).
- Denetçiler arasındaki koordinasyon ve işbirliği, etkili kurumsal yönetişim anlayışına katkı sağlar (Gramling vd., 2004, s.194). Açık ve samimi ilişkiler, kamuyu aydınlatma ilkesi çerçevesinde finansal tabloların kalitesine olumlu şekilde yansır (Mihret & Admassu, 2011, s.67).

### 2.15. İç Denetim ve Teknoloji İlişkisi

Bilgi teknolojilerinin inanılmaz bir hızla gelişmesi, yaşamımızın her alanını derinden etkilemiştir. Artık insan yaşamının tüm faaliyetlerinde; uzay çalışmalarından eğitime, tıptan sinemaya, tarımdan sanayiye kadar birçok alanda teknolojiden faydalanılmaktadır. Ev hanımlarından astronotlara kadar herkes teknolojiye ihtiyaç duymaktadır. Bu ihtiyacı en yoğun şekilde hisseden kesimlerden biri de işletmelerdir. Artık çağdaş işletmeler üretim, pazarlama, insan kaynakları ve muhasebe dahil birçok faaliyetini bilgisayarla yapmaktadır. Bunun da ötesinde, işletmeler bilgisayarı karar almada etkin şekilde kullanmaktadır. Böylece bilgiler doğru, güvenilir ve tutarlı bir temelde hızla işlenebilmekte, hem muhasebe fonksiyonu hem de yönetimin diğer karar alma dayanakları güçlenerek karar alma süreci çabuklaşmaktadır (Erdoğan, 2005, s. 137).

IIA 1941 yılında kurulduğu zaman kişisel bilgisayarlar ve internet yoktu, sivil bireyler arasında açık küresel bir iletişim ağı bir hayaldi. Günümüze baktığımızda ise

teknolojik yenilikler çok hızlı ve hayatımızın neredeyse bütün yönlerini etkilemektedir. Giderek hızlanan dijitalleşmenin ve Endüstri 4.0'ın getirdiği 'Nesnelerin İnterneti' kavramının şekillendirmesiyle, insanlar ve makineler her geçen gün daha fazla birbirine bağlı hale gelmektedir. Günümüzde neredeyse bütün işletmelerin merkezinde teknoloji yer almaktadır. İşletmeler hem faaliyetlerini sürdürmek hem de yenilikler (ürün, üretim süreci, yönetim tarzı vb.) geliştirmek ve gelecekte başarıyı mümkün kılmak için bilgi teknolojilerine bağımlıdırlar. Hiç şüphesiz dijital çağdaki keskin teknolojik değişim, çeşitli sektörlerdeki işletmeler için daha önce hayal bile edilemeyen yeni bir dünya yarattı. Fakat bu işletmeler, daha önce hiç olmadığı kadar geniş ve güvenilmez bir risk ortamıyla da karşı karşıya kaldılar (Protiviti, 2016, s. 3).

İşletmelerin hemen her kademesinde bilgisayar sistemlerinden giderek daha fazla yararlanılması iç denetimi risk denetimi açısından karmaşıklaştırmaktadır. Ancak bilgisayarlar ve giderek gelişen denetim yazılımları denetçilerin işlerini kolaylaştırmaktadır. İç denetim birimlerinde riskleri izlemek, gereksiz işlemleri tespit etmek, eğilimleri ve sapmaları ortaya çıkarmak üzere verileri analiz etmek ve iç denetim biriminin verimliliğini artırmak amacıyla BT'den yararlanılmaktadır. Örneğin çok yıllı denetim planları güncellenirken; özel faaliyetlerle ilişkili risk faktöründeki değişim izlenirken; denetim programlarına, el kitaplarına ve talimatlara ulaşılırken; çalışma kâğıtları hazırlanırken ve denetim birimiyle merkezden uzakta bulunan denetçilerle iletişim kurulurken BT'den faydalanılabilir. (Yetiş, 2001, s.3). BT'leri, denetim sürelerini ve maliyetlerini azaltmıştır.

Teknoloji beraberinde bazı riskleri de getirmiştir. Örneğin, yeterli planlama ve risk yönetimi olmadan bir e-ticaret projesi bile zararla sonuçlanabilir. Şirketlerin işlerini çok hızlı yönettiği günümüz iş dünyasında, iç denetçilerin sağduyulu davranarak risk yönetimini dikkate almaları gerekir (Mcnamee & Chan, 2002, s. 39).

Teknoloji, iç denetim birimlerine daha üretken ve güçlü bir öngörü yeteneğine sahip olunmasında ve en ayrıntılı düzeydeki işlerin izinin sürülmesinde katkı sağlar. Teknoloji, küresel işletmeleri daha derinden etkilemiştir. Bu işletmelerde iç denetim birimi daha fazla yeni taleple karşı karşıya kalır. Örneğin, iç denetçiler bir uygulamada ya da sistemin tamamında yürütülen işlerde ortaya çıkabilecek potansiyel riskler ve teknolojiler hakkında her şeyi bilmelidirler (Protiviti, 2016, s. 3). İşletmenin yönetişim, risk yönetimi ve uygunluk faaliyetlerinin, bunların çevresinde dönen diğer fonksiyonlarla beraber ele alınmasını öngören YRU yaklaşımı (Governance-Risk Management-Compliance (GRC))

ve bu yaklaşımdan hareketle geliştirilen güvence yazılımlarının işletmede geliştirilmesinde ve kullanılmasında, iç denetçilere işletme içerisinde sahip oldukları eşsiz konum sebebiyle büyük görevler düşmektedir. Günümüz iç denetçileri bu görevi hakkıyla yerine getirebilmek amacıyla hem YRU yaklaşımının anlaşılması hem de işletmenin teknoloji altyapısıyla uyumlaştırılması konusunda kendilerini yeterli seviyeye getirecek yeteneklere sahip olmaya çalışmalıdırlar. 2017 YRU için teknoloji dönüşüm yılı olarak görülmektedir.[2] Bu açıdan bakıldığında, YRU hakkında bilgi sahibi olmayan iç denetçiler, geleceğin iç denetim dünyasında kendilerine yer bulamayacaklardır.

Uluslararası İç Denetim Standartlarına göre iç denetçilerin gelecekteki sorumluluklarını hakkıyla üstlenebilmeleri için teknoloji ile ilgili konularda belirli bir yeterlikte olmaları gerekmektedir. Standart 1210.A3'e göre, "İç denetçiler, verilen görevi yerine getirebilmek için bilgi teknolojileri ve kontrolleriyle ilgili kilit bilgilere ve mevcut teknoloji tabanlı denetim tekniklerine sahip olmalıdır. Ancak, bütün iç denetçilerden asıl sorumluluğu bilgi teknolojilerinin denetimi olan denetçiler kadar uzmanlığa sahip olmaları beklenmez." Standartta belirtildiği üzere, denetçilerin teknolojiyle ilgili konularda asgari bilgi düzeyine sahip olmaları ve denetim ekiplerinde bu konuda bir uzman denetçi bulundurulması gerektiği çok açıktır (Switzer, 2007, s. 45).

Artık içinde bulunduğumuzu söyleyebileceğimiz 4. Endüstri çağıyla beraber hem muhasebenin hem yönetim fonksiyonunun hem de denetimin iş tanımı giderek değişecektir. Yönetim ve muhasebe, daha önce insan gücüyle yürüttüğü, gündelik rutin karar alma gibi birçok çabasını tamamen bilgisayarlara bırakacaktır. Zaten daha önce defter tutma fonksiyonunu çeşitli yazılımlara bırakan muhasebe bilimi, artık veri çözümleme süreçlerini de bilgi teknolojilerine bırakacak, sadece önüne çoğunlukla otomatik bir şekilde gelen işlenmiş verileri yorumlayacaktır. İç denetim mesleği ise, otomatik şekilde tutulan kayıtların ve bilgi teknolojileri ortamında yürütülen işlerin doğruluğunu bilgisayarlar aracılığıyla test edecek ve işletmenin gerek raporlama gerek muhasebe dışındaki işlerinin güvenli bir şekilde yerine getirilmesinden sorumlu olacaktır.

Finansal ve operasyonel sistemlerini otomatikleştirmek için veri işleme araçlarına önemli miktarda yatırım yapan işletmelerin sayısı her geçen gün artmaktadır. Veri işleme sistemleri, gitgide karmaşıklaşmaktadır. Sonuç olarak, işletme yönetimleri ve denetim komiteleri, iç denetçilerinden bilgisayar sistemlerinin sistem geliştirme yaşam

[2] Ayrıntılı bilgi için bakınız: http://www.corporatecomplianceinsights.com/2017-a-transformational-year-for-grc/

döngüsünün bir parçası olmalarını istemektedir. İç denetçilerden aşağıda sıralananları inceleyerek sistemlerinin etkinliğini bağımsız bir şekilde değerlendirmelerini istemektedirler (Gupta & Ray, 1998, s. 7):

- Sistemin yeterliliğiyle işletmenin ihtiyaçlarının uygunluğu;
- Zamanında kurulum;
- Bütçe maliyetleri ve maliyet aşımları;
- Operasyonel ve finansal kontrollerin yeterliliği;
- Sistem sürdürülebilirliği.

Ayrıca, iç denetçilerden giderek daha fazla mikrobilgisayar ortamı, servis merkezi, toplu sistemler, dağıtılmış sistemler, çevrimiçi ve gerçek zamanlı sistemler ve veri tabanı sistemleri gibi bir dizi elektronik veri işleme (EDP) ortamında denetim yapmaları beklenmektedir. Birçok şirketin çevresi daha fazla bilgisayarlı hale geldikçe, bu ortamda denetim için iç denetçilere daha fazla ihtiyaç duyulmaktadır. Veri işleme sistemlerini denetlemekle birlikte geleceğin iç denetçisi, yalnızca şirket politikalarına ve yordamlarına uyulmasını sağlamamalı veya hileyi ortaya çıkarmak amacıyla çalışmamalı, aynı zamanda sistem kontrollerini, sistemin güvenilirliğini ve maliyet etkinliğini denetlemelidir. Bu bağlamda, Reeve (1990, s. 22) şunları gözlemlemektedir:

Gelecekte iç denetçiler güçlü bir elektronik veri işleme çalışma bilgisine sahip olacaklar, böylece denetim testleri çok daha verimli şekilde yapılabilecektir. Denetimlerde kullanılan yazılım programları, özellikle veri tabanlarının denetim testlerinin daha yüksek performansı için tasarlanacaktır. Sınırlayıcı faktörler koyma ve diğer veri dosyalarıyla çapraz kontroller yapma gibi iç kontroller, yönetim tarafından kullanılan yazılım kontrollerine dâhil edilecektir.

Gelecek yıllarda, denetim müşterileri (yani işletmeler) kâğıtsız sistemlere geçtikçe ve denetçilerin çevrimiçi olarak çoğu yordamı yerine getirmesine imkân veren denetim yazılımları geliştirildikçe kâğıtsız denetimler yaygınlaşacaktır. Geçmişe göre günümüzde bilgisayarların disk depolarının hacmi ve elektronik olarak yapılan işlemelerin sayısı giderek artmaktadır. Elektronik veri değişimi (EDI), görüntü işleme ve elektronik dosya transferi gibi teknolojiler, geleneksel denetim kayıtlarını ortadan kaldıracaktır. Bu teknolojiler, geleneksel olarak kâğıt formunda kaynak belgelere dayanan denetim sürecinin doğasını büyük ölçüde değiştirecektir. Çevrimiçi (On-line) sistemleri denetlemek için, denetçiler, çevrimiçi denetim yazılımını birincil denetim aracı olarak kullanmalı ve kanıtları elektronik olarak toplamalıdırlar. Bu teknolojinin kullanılması,

denetçiyi birçok sıradan denetim görevinden kurtaracak ve denetçinin zamanını müşterinin işini anlama ve çeşitli riskleri değerlendirmek gibi üst düzey görevler için kullanmasına izin verecektir (Bierstaker vd., 2001, s. 159).

Gelecek ne gösterir? Kimse emin olamaz, fakat iç denetçiler eğer işletmelerinin değer katan bir ortağı olarak tanınmayı umuyorlarsa, geleceğin getirdiği şeylerin avantajlarını elde etmek için daha iyi bir konuma sahip olmak zorundadırlar. İşletmenin yapısına ve performansına yönelik eleştirel ve yapıcı değerlendirmeler yapmak amacıyla bilgisayar kaynaklarını verimli bir şekilde kullanmak, günümüzde tüm denetçiler için bir görevdir (Coderre, 2009, s. 102).

## 2.16. İç Denetim ve İç Kontrol İlişkisi

İç denetim, esas itibariyle işletmenin iç kontrolünün amaçlandığı şekilde çalışıp çalışmadığını inceleyen ve üst yönetime raporlayan bir işlev üstlenir. İç denetim, üst yönetimin görev ve sorumluluklarını yerine getirmesine yardım eder. İç denetçi, iç kontrolü değerlendirerek, işletmenin amaçlarına etkin ve verimli bir şekilde ulaşıp ulaşmayacağı konusunda iç kontrolün yeterli güveni sağlaması için gerekli önlemlerin alınmasını sağlar.

1992 yılında yayınlanan COSO Raporu, iç denetçilerin işletmenin iç kontrolünün kurulmasında ve etkin bir şekilde işleyip işlemediğinin değerlendirilmesinde önemli bir role sahip olduğunu vurgular. Bir işletmede iç kontrolün kurulmasından ve etkin bir şekilde işlemesinden sorumlu olan üst yönetim, iç kontrollerin kalitesi hakkında bilgiyi, aynı zamanda iç kontrolün bir parçası olan iç denetimin raporlarından elde edebilir. İç denetim, iç kontroller hakkında yönetime bilgi sağlar, değerlendirmelerde bulunur ve tavsiyeler sunar. Bu yüzden, iç kontrol bir iç denetçinin anlaması gereken en önemli kavramlardan biridir (Kurnaz & Çetinoğlu, 2010, s.40).

### 2.16.1. İç kontrol kavramı

Günümüzde evrensel boyutta kabul gören COSO'nun iç kontrol tanımından önce farklı kişiler ve organizasyonlar tarafından birçok iç kontrol tanımı yapılmış ve kontrol modelleri önerilmiştir.

Viktor Z. Brink 1946 yılında yayımlanan iç denetçi başlıklı makalesinde etkin bir iç kontrolün kapsamını tanımlamıştır. Buna göre etkin bir iç kontrolün başlıca bileşenleri; zamanında bilgi ulaştıran iyi bir muhasebe sistemi, muhasebenin de ötesinde yazılı halde

politika ve yordamlar, faaliyetlerin etkinliğini ölçmek için kullanılan iyi düzenlenmiş bütçeler ve iç denetimdir (Uzay, 1999, s.7).

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununda iç kontrol;

"*İdarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik, verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, mali ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yönetim ve süreçle, iç denetimi kapsayan mali ve diğer kontroller bütünü*"

olarak tanımlanmıştır.

Evrensel kabul gören COSO tanımından önce, uygulamaya yönelik en kapsamlı tanımlar AICPA tarafından yapılmıştır. 1992 yılında COSO çerçevesi yayımlanmadan önce, denetim uygulamalarında AICPA'nın iç kontrol yaklaşımları etkili olmuştur. AICPA, 1949'da iç kontrolü şöyle tanımlamıştır (Cömert, 2016, s. 7);

"*İç kontrol, işletmede varlıkların korunması, muhasebe verilerinin doğruluğu ve güvenilirliğinin sağlanması, faaliyetlerin etkili biçimde yürütülmesinin teşviki ve yönetsel politikalara bağlılığın özendirilmesi için kabul edilen tüm eşgüdüm, yöntem ve önlemleri ile organizasyon planından ibarettir.*"

IIA'nın 1999 yılında yaptığı tanıma göre;

"*İç kontrol, bir örgüt yönetiminin ayrılmaz bir parçası olup; faaliyetlerde etkinlik ve verimlilik, bütçenin uygulanması, finansal tablolar ile ilgili raporlar dâhil olmak üzere finansal raporlama ve iç ile dış kullanıma ilişkin diğer raporların güvenilirliği, yürürlükteki yasalara ve düzenlemelere uygunluk amaçlarının gerçekleştirilmesi konusunda makul bir güvence sağlayan, organizasyon faaliyetlerinde devamlılık temelinde bir seri eylem ve aktivitedir*".

İç kontrolün günümüzde en fazla kabul gören tanımı, Treadway Komisyonu tarafından kurulan COSO'nun (The Committee of Sponsoring Organizations) yaptığı tanımdır. COSO; işletme etiği, etkili iç kontroller ve kurumsal yönetişim yoluyla finansal raporlamanın kalitesinin artırılması amacıyla çalışan bir özel sektör organizasyonudur ve iç denetim odaklı faaliyetlerin yürütülmesi amacıyla iç denetçilerin kullanması için ölçütler tanımlar. COSO, İç Kontrol – Bütünleşik Çerçeve Raporunda iç kontrolü şöyle tanımlamıştır (Reding vd., 2013, s.6-8):

"*İç kontrol; işletmenin yönetim kurulu, yöneticileri ve diğer personeli tarafından etkilenen ve faaliyetlerin etkinliği ve verimliliği, finansal raporlamanın güvenilirliği, ilgili yasalara ve düzenlemelere uygunluk olarak sınıflandırılan işletme amaçlarına ulaşmak için makul güvence sağlamak üzere tasarlanan bir süreçtir.*"

COSO iç kontrol tanımıyla, iç kontrolün amaçlarını ve performansını açıklayan anahtar kavramları belirlemiştir (Kagermann vd., 2008, s.6):

- İç kontrol bir süreçtir. Devam eden görevler ve faaliyetlerden oluşur. İç kontrol hiçbir zaman bitmez ve sürekli olarak tekrar eder.
- İç kontrolden kesin bir güvence sağlaması değil, sadece makul seviyede bir güvence sağlaması beklenebilir.
- İç kontrol sadece politika ve yordamları belirleyenler tarafından değil, işletmenin tüm seviyelerinde yer alan çalışanların eylemlerinden etkilenir.
- İç kontroller birbirleriyle örtüşen ve birbirlerini etkileyen alanlarda (faaliyet, raporlama, uygunluk) bir ya da daha fazla farklı amaca ulaşılması için düzenlenir.
- İç kontroller işletmenin tamamında ya da bir bölümünde, bir faaliyet biriminde ve bir işletme sürecinde uygulanabilir.

İç kontrol, yönetime işletmenin amaçlarına ulaşmasında makul güvence sağlamak amacıyla tasarlanmış politika ve yordamlardan oluşur. Yönetim, işletmede etkili bir iç kontrolün tasarlanması noktasında üç genel amaca sahiptir (Arens vd., 2012, s.290):

1. Finansal Raporlamanın Güvenilirliği: Yönetim; yatırımcılar, kredi kuruluşları ve diğer finansal tablo kullanıcıları için finansal tabloların hazırlanmasından sorumludur. Yönetim, hem yasal hem de mesleki sorumlulukları gereğince, finansal bilginin Genel Kabul Görmüş Muhasebe İlkeleri ve Uluslararası Finansal Raporlama Standartları gibi muhasebe çerçevelerinin raporlama gerekliliklerileyle uyumlu bir şekilde, dürüstçe sunulduğundan emin olmak zorundadır. Etkili iç kontrolün finansal raporlama konusunda amacı, işletmenin finansal raporlama sorumluluklarının yerine getirilmesidir.
2. Faaliyetlerin Etkinliği ve Verimliliği: İşletmedeki kontroller, kaynakların işletmenin amaçları doğrultusunda, etkin ve verimli bir şekilde kullanılmasını destekler. Bu kontrollerin en önemli amaçlarından biri, karar alma sürecinde kullanılmak üzere işletmenin faaliyetleri hakkında finansal ve finansal olmayan bilginin doğruluğunun sağlanmasıdır.
3. Yasalara ve Düzenlemelere Uygunluk: Yasalar, halka açık işletmelerin yönetimlerinin iç kontrolün finansal raporlama üzerindeki etkinliği hakkında bir raporu kamuoyuyla paylaşmalarını zorunlu tutmaktadır. Ayrıca işletmelerin halka açık olsun ya da olmasın -hatta kar amacı gütmeyen kurumların bile- birçok yasaya ve düzenlemeye uymaları gereklidir. Öyle ki, bu yasaların bazıları çevrenin korunması ve insan hakları gibi muhasebeyle ilişkili olmayabilir ya da vergi düzenlemeleri ve yolsuzluğu önleme gibi muhasebeyle yakın ilişkili olabilir.

### 2.16.2. Yönetimin ve iç denetimin iç kontrol sorumlulukları

İşletmede iç kontrolün kurulmasından ve etkili bir şekilde işletilmesinden yönetim sorumludur. İç kontrol hakkında uygun politikalar geliştirmelidir ve iç kontrole ilişkin riskleri göz önünde bulundurarak, iç kontrolün etkinliğini geliştirecek şekilde belirlediği politikaları uygulamalıdır (Financial Reporting Council, 2005, s.6). Yönetimin iç kontrole ilişkin sorumlulukları şöyle özetlenebilir (Pickett, 2010, s.249):

- Kontrole ihtiyaç duyulan alanları belirlemek;
- İşletme için uygun kontrolleri tasarlamak;
- İşletme için geliştirilen kontrollerin uygulanmasını sağlamak;
- Kontrollerin gerektiği gibi uygulanıp uygulanmadığını incelemek;
- Gelişen ihtiyaçlar ve değişen işletme ortamına uygun şekilde kontrolleri güncellemektir.

Yönetimin iç kontrole ilişkin sorumlulukları yerine getirmesinde en önemli destekçisi iç denetçidir. İç kontrolün geliştirilmesi amacıyla iç denetçi, yönetsel bir sorumluluk üstlenmeden sorumluluklarını yerine getirmesinde yönetime destek olmalıdır. Performans Standardı 2120, iç denetçinin, kontrollere ilişkin görevlerini düzenlemektedir. İç denetim, kontrollerin etkinlik ve verimliliğini değerlendirerek ve sürekli gelişimini destekleyerek, işletmenin etkin işleyen bir iç kontrole sahip olmasını sağlamalıdır.

Daha önce de ifade ettiğimiz gibi, iç denetim iç kontrolün başlıca unsurlarından birisidir. İç kontrolün değerlendirilmesi ve geliştirilmesi iç denetçilerin asıl görevidir. İç denetim, iç kontrolün bir parçası olarak, bir veya birçok faaliyetin etkin ve verimli yürütülmesi amacıyla ortaya çıkmadan önce olumsuz bir durumu engellemek ya da ortaya çıkan olumsuzlukların tekrar etmemesinden emin olmak gibi amaçlara sahip olan kontrollerin geliştirilmesini sağlamalıdır. İç denetçiler, kontrolleri, geliştirilme amaçlarıyla birlikte ele almalı ve işletme içinde herhangi bir kontrol zafiyetinin yaşanmaması için uyanık olmalıdır. Ayrıca iç denetçiler, kontrollerin değerlendirilmesi için uygun ve yeterli ölçütlere sahip olmalıdırlar. Bu ölçütlerin geliştirilmesi için, gerekli görülürse yönetimle birlikte çalışılmalıdır.

COSO, iç kontrolü beş bileşene ayırarak inceler. İç denetim, iç kontrol bileşenlerinin etkinliği ve verimliliğini değerlendirmek ve geliştirmek noktasında, aynı zamanda iç kontrolün bir parçası olarak sorumluluklara sahiptir. İç denetçiler, kontrol ortamının oluşturulmasında, örneğin dürüstlük ve etik değerlerin geliştirilmesinde veya

yeterli seviyede belgelendirme yapılması gibi, bir kontrol faaliyetinin oluşturulmasında nihai sorumluluğa sahip olan yönetimin en büyük destekçisidir. Ayrıca iç denetçiler kontrollerin değerlendirilmesi ve geliştirilmesi sürecinde, kontrolün etkinliği için bilginin hiyerarşik basamaklar arasında yatay ve dikey olarak iletilmesinin sağlanmasında ve işletmenin maruz kaldığı risklere bağlı olarak kontroller geliştirilmesinde yönetime yol gösterir.

İç denetim, esas itibariyle iç kontrolün etkin ve verimli çalışıp çalışmadığını inceleyen ve geliştirme önerileriyle birlikte yönetime rapor veren bir işlev üstlenir. Bu işlevi, iç kontrolü sürekli devam eden bir temelde izleyerek yerine getirmelidir. Bu bağlamda, iç kontrolün operasyonel olarak bağımsız ve gerekli mesleki uzmanlığa sahip çalışanlardan oluşan etkili ve kapsamlı bir iç denetim unsuruna sahip olması gereklidir. İç kontrolün izlenmesinin bir parçası olarak iç denetim; tespit ettiği kontrol eksikliklerini uygun seviyedeki yöneticilere zamanında raporlamalı ve kesin bir şekilde giderilmesini sağlamalıdır.

### 2.16.3. Yönetsel kontroller ve muhasebe kontrolleri

Geniş anlamda iç kontrol; muhasebe kontrolleri ve yönetsel nitelikteki kontrollerden oluşur.

Yönetsel kontroller; işletme faaliyetlerinin etkinliğini ve verimliliğini, yönetimin politikalarına bağlılığı artırma amaçlarına yönelik olarak işleyen fakat finansal kayıtlarla doğrudan ilişkisi olmayan tüm yöntem, yordam ve organizasyon planını kapsar. Bir işletmenin pazarlama personelinin yaptığı temasları, aldığı siparişleri, iadeler ve nedenlerini gösteren bir raporu, merkez büroya göndermelerini sağlayan bir politikanın uygulanması örneğinde olduğu gibi mali nitelikli olmayan faaliyetlerden oluşur (Güredin, 2000, s.166).

Yönetsel kontroller, örgütsel amaçlara ulaşmak için yönetimin sorumluluklarından oluşur. Yönetimin kararlarına temel oluşturacak olan kayıtlama fonksiyonları ve süreçlerini içerir. Yönetsel kontroller, faaliyetlerin etkinliğini arttırır ve yönetim politikalarına bağlılığı sağlamaya yöneliktir. Daha ayrıntılı ifade etmek gerekirse aşağıdaki kontroller yönetsel kontrollerin kapsamındadır (Yılancı, 2003, s.34):

- Faaliyetlerin yönetim politikalarına, planlarına, yasalara ve düzenlemelere uygunluğunun sağlanması,
- Kaynakların ekonomik ve verimli kullanılması,

- Belirlenmiş faaliyet amaçlarına ulaşılması ile ilgili usul ve yöntemlerin uygulanması.

Muhasebe kontrolleri ise; varlıkların korunması ve finansal kayıtların güvenilirliğiyle doğrudan ilgili tüm yöntem ve yordamları kapsar. Genel olarak yetkilendirme ve onaylama, kayıt tutma ve muhasebe raporlarının hazırlanması ile ilgili görevler, varlıkların korunması ve varlıklar üzerindeki fiziki kontroller ve iç denetim görevlerinin belirlenmesi ile ilgili kontrol önlemlerinden oluşur. Ödemeleri yapacak personel ile parasal işlemleri kaydedecek personelin görevlerinin ayrımı örneğinde olduğu gibi finansal nitelikli faaliyetlerdir.

Muhasebe kontrolleri ve yönetsel kontroller arasında çoğu durumda kesin sınırlar bulunmaz. Yönetsel kontrollerin kapsamında yer alan bazı kayıt ve yordamlar, aynı zamanda muhasebe kontrolleriyle de ilgili olabilir. Mamullere göre sınıflandırılan satış ve satış maliyeti kayıtları, hem muhasebe hem de yönetsel kontroller ile ilgilidir. Benzer şekilde, bazı yönetsel yordamlar muhasebe kontrollerini ilgilendirebilir. Örneğin, yatırım projelerinde olduğu gibi (Kepekçi, 1994, s.6).

### 2.16.4. Önleyici kontroller, bulma kontrolleri ve düzeltici kontroller

Kontroller, çeşitli birimlerde uygulanmak amacıyla tasarlanabilir. Bazıları ortaya çıkmadan önce istenmeyen sonuçları önlemek için geliştirilir (Önleyici Kontroller). Bazıları ortaya çıktıklarında istenmeyen sonuçların belirlenmesi için tasarlanır (Bulma Kontrolleri). Bazılarıysa istenmeyen sonuçlara karşı düzeltici eylemlerde bulunulduğundan ya da istenmeyen sonuçların tekrarlanmamasından emin olmak için tasarlanır (Düzeltici Kontroller). Bu kontroller aşağıda açıklanmıştır (Sawyer vd., 2005, s.72).

Önleyici kontroller hatayı önler ve düzeltme maliyetleriyle karşılaşılmamasını sağlar. Önleyici kontroller, bulma kontrollerinden daha az maliyetlidir. Önleyici kontrol örnekleri şunlardır; kasıtlı olarak yapılan yanlışları önlemek için görevlerin uygun şekilde ayrılması, işletmenin kaynaklarının uygun olmayan şekilde kullanılmasının önüne geçmek için uygun yetkilendirmeler yapılması, hatalı işlemleri önlemek için bilgi teknolojilerinden yararlanılarak geliştirilen kontroller ve kötüye kullanımına engel olmak için varlıklar üzerindeki fiziksel kontroller. Bir işletmede satın almadan önce satın alma isteğinin bir onay sürecinden geçirilmesi veya sisteme/uygulamalara yetkisiz erişimlerin önlenmesi için şifreler kullanılması önleyici kontrollere örnektir.

İşletmede etkin işleyen önleyici kontrollerin geliştirilmesine özen gösterilmesi, iç kontrolün etkinliği açısından bulma veya düzeltici kontrollere göre daha doğru bir yaklaşımdır. Çünkü önleyici kontroller bir hata, hile veya herhangi bir olumsuzluğun iç kontrole girmeden önce engellenmesini sağlar. Çoğu zaman hata, hile veya herhangi bir olumsuzluğun eyleme geçtikten sonra tespit edilmesi veya verdiği tahribatın ortadan kaldırılması ve tekrar etmemesinin sağlanması daha maliyetli ve karmaşık işlemleri gerektirir. Bu sebeple kontroller geliştirilirken çöp giren çöp çıkar (Garbage in garbage out) anlayışıyla hareket edilmesi gerekir.

Bulma kontrolleri, genellikle önleyici kontrollere göre daha fazla maliyetlidir, ancak iç kontrol sisteminin etkinliği için bu kontroller de gereklidir. Çünkü bulma kontrolleri, önleyici kontrollerin etkinliğini ölçer. Ayrıca bazı hata ve hileler sistem tarafından önlenemeyebilir ve yapıldıkları zaman ortaya çıkarılmaları gereklidir. Bulma kontrolleri, performansın kaydedilmesi ve bağımsız bir şekilde kontrol edilmesi gibi incelemeleri ve karşılaştırmaları içerir. Ayrıca, banka hesaplarındaki nakit miktarının mutabakatı, alacak hesaplarının müşteriler ile iletişim kurularak doğrulanması, stokların fiziksel miktarının sayılması ve varyans analiziyle incelenmesi, borç hesaplarının tedarikçiler aracılığıyla doğrulanması ve bilgi teknolojilerinin incelenmesi bulma kontrollerinin kapsamındadır. Bir işletmede bordro raporlarının incelenmesi veya hasar kanıtı elde etmek için bilgi sisteminde otomatik olarak kaydedilen log dosyalarının incelenmesi bulma kontrollerine örnektir.

Düzeltici kontroller istenmeyen sonuçlar ortaya çıktığında veya bir hata ve hile bulunduğunda ön plana çıkar. Bütün bulma kontrolleri, saptanan eksiklikler giderilmediği veya olumsuzluğun yeniden meydana gelmesine izin verildiği sürece değersizdir. Bu yüzden yönetim istenmeyen durumları ortadan kaldırmak ve yeniden tekrar etmesine engel olmak amacıyla yordamlar geliştirmelidir. Belgelendirme ve kaydetme sistemleri problemler çözülünceye veya düzeltilinceye kadar yönetimin gözetimi altında problemleri kaydetmelidir. Bu nedenle, düzeltici kontrollerin problemleri önlemeyle başlayan ve düzeltmek için bulmayla devam eden bir döngüyle yakın ilişki içinde olduğu söylenebilir. İşletmede çalışanların sorumlulukları değiştiğinde, bilgi teknolojileri erişim listelerinin değiştirilmesi düzeltici kontrollere örnektir.

### 2.16.5. Bilgi teknolojilerinin iç kontroller üzerindeki etkisi

Bilgi teknolojileri verilerin kaydedilmesi, depolanması ve belirli süreçlerden geçirilerek bilgiler üretilmesi, üretilen bilgilere erişim ve bilgi transferi gibi işlemlerin daha hızlı, etkili ve verimli yapılmasını sağlar. Bilgi teknolojileri ortamında yaşanan hızlı değişim ve gelişmeler, işletmeleri ve işletme çevresini derinden etkilemiştir. Bilginin eş zamanlı olarak dünyanın değişik yerlerinde bulunan farklı taraflarla karşılıklı paylaşımına olanak tanıyan birçok teknolojik yenilik, günümüzde işletme faaliyetlerinin tamamının ya da bir kısmının elektronik ortamda yürütülmesine yol açmıştır (Önce & İşgüden, 2012, s.40).

İşletmede bilgi teknolojileri kullanımının; işlemlerin yetkilendirilmesi, kaydedilmesi, yürütülmesi ve raporlanması süreçlerini derinden etkileyeceği için, iç kontroller üzerinde güçlü bir etkiye sahip olduğu söylenebilir. BT, iç kontrolün oluşturulması, işleyişi ve amaçlarına ulaşmasında oynadığı temel rol aracılığıyla iç kontrol sistemini birçok noktadan teknolojik bir ağ olarak sarmakta ve hem içsel hem de çevresel oluşumunda teknolojik yapının öngörülmesini zorunlu kılmaktadır (Erdoğan, 2012, s.112). Birçok bilgi sisteminde, iç kontrol çoğu zaman birbirinden bağımsız otomatik ve manuel kontrollerin bir kombinasyonundan oluşur. Manuel kontroller, genellikle BT tarafından üretilen bilgiyi kullanır ve çoğu zaman otomatik kontroller tarafından tespit edilen hataları ve aykırılıkları izleme fonksiyonuna yön verir. Bir işletmede, manuel ve otomatik kontrollerden ne kadar faydalanılacağı, işletmede kullanılan BT'nin yapısı ve karmaşıklığına bağlı olarak değişir. Örneğin, işletmede bulut bilişim kullanılıyorsa ve veri bulutta depolanıyorsa, bu durum kendine has risklere ve uygun kontrol ihtiyacına yol açar.

İç kontrol üzerindeki riskler işletme bilgi sisteminin yapısına ve özelliklerine bağlı olarak değişir. Örneğin, birden çok kullanıcının ortak bir veri tabanına erişebildiği bir durumda, kullanıcı girişi üzerinde bir kontrol noktası geliştirilmez ise, işletmenin veri tabanı güvenliği riske atılmış olacaktır. Bu durum verinin uygunsuz biçimde değiştirilmesine veya tahrip edilmesine yol açabilir. BT çalışanları veya kullanıcılar, atandıkları görevi yürütmek için ihtiyaç duyduklarının ötesinde erişim ayrıcalıklarına sahip olurlarsa, bu durum görevlerin ayrılığını bozar ve yetkisiz işlemlerin yapılmasına ve verinin değiştirilmesine yol açar. BT'nin işletmenin iç kontrolü üzerindeki potansiyel faydaları ve sebep olabileceği riskler Tablo 2.5'te yer almaktadır (Messier vd., 2016, s.181):

**Tablo 2.5.** *İç Kontrolde Bilgi Teknolojilerinin Faydaları ve Riskleri (Sawyer, Dittenhofer, Scheiner, 2005, s. 7-8)*

| |
|---|
| ***Faydalar*** <br> • Önceden tanımlanmış işletme kurallarına tutarlı bir şekilde uyulmasını sağlar ve yüksek hacimli işlemlerin veya verinin işlenmesinde karmaşık hesaplamaları yapar. <br> • Bilginin zamanlılığını, elde edilebilirliğini ve doğruluğunu artırır. <br> • Bilginin karar alma için gerekli olan ek analizlerini kolaylaştırır. <br> • İşletmenin faaliyetlerini, politikalarını ve yordamlarını izleme yeteneğini geliştirir. <br> • Kontrollerin hata ve hileleri bulma ve önleme gücünü geliştirir. <br> • Uygulamalardaki, veri tabanındaki ve faaliyet sistemlerindeki güvenlik kontrolleriyle görevlerin uygun biçimde ayrılmasını sağlar. |
| ***Riskler*** <br> • Doğru veri işleyip işlemediği yönetim tarafından doğrulanamayan sistem veya programlara aşırı güven duyulmasını sağlayabilir. <br> • Aslında olmayan işlemlerin yetkisi olmayan çalışanlarca kaydı gibi veri üzerinde uygun olmayan değişikliklere veya verinin tahrip edilmesine sebep olabilecek yetkisiz erişimlere yol açabilir. <br> • Ana dosyalardaki veri, yetkisiz şekilde değiştirilebilir. <br> • Sistemler veya programlar yetkisiz şekilde değiştirilebilir. <br> • Veri kayıpları yaşanabilir. <br> • Uygun olmayan manuel müdahaleler olabilir. <br> • Sistemler veya programlarda ihtiyaç duyulan değişiklikler yapılamayabilir. |

### 2.16.6. İç kontrol çerçeveleri

İç kontrole yönelik çeşitli çerçeveler ve raporlar hazırlanmış olup, şu anda dünyada en fazla kabul gören ve uygulanan çerçeve, 1992 yılında hazırlanan COSO İç Kontrol Çerçevesidir. COSO çerçevesi dışında CoCo Çerçevesi, Turnbull Raporu ve bilgi teknolojileri alanına yönelik olarak geliştirilen COBIT Çerçevesi yaygın olarak kullanılan diğer çerçevelerdir (Pehlivanlı, 2010, s.31).

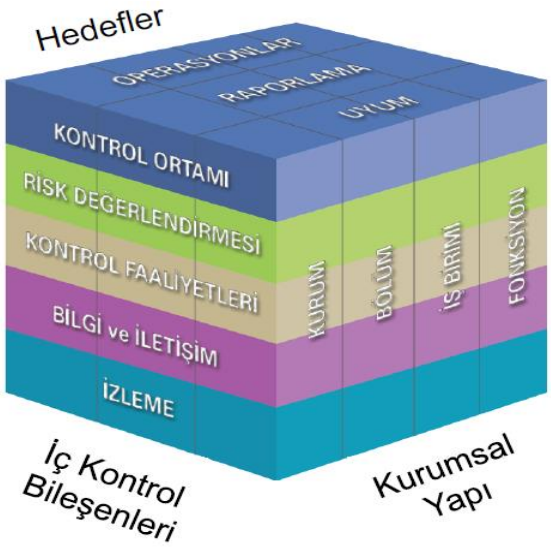
#### *2.16.6.1. COSO çerçevesi*

COSO (The Committee of Sponsoring Organizations) hileli finansal raporlamaya neden olabilen faktörler hakkında çalışmalar yapmak ve raporlar hazırlamaktan sorumlu olan Hileli Finansal Raporlama Ulusal Komisyonuna destek olmak amacıyla 1985 yılında AICPA (American Institute of Certified Public Accountants), AAA (American Accounting Association), FEI (Financial Executives International), IIA ve IMA (Institute of Management Accountants)'nın desteğiyle kurulmuştur. Zaman içerisinde COSO ilk kuruluş amacının yanında, misyonunu finansal raporlamanın kalitesini artırmak yönünde

genişletmiştir. COSO bu misyonunun önemli bir parçası olarak iç kontrol için bir rehber geliştirmeyi amaçlamıştır. 1992 yılında COSO, işletmeler ve diğer kurumların iç kontrollerini değerlendirmek amacıyla kullanabilecekleri bir çerçeve geliştirmiş ve İç Kontrol – Bütünleşik Çerçeve adıyla yayımlamıştır (Graham, 2015, s.2).

COSO Çerçevesi, iç kontrol hakkında geliştirilen diğer çerçeve ve raporlara yön verir. Ayrıca Uluslararası İç Denetim Standartları, AICPA tarafından yayımlanan Denetim Standartları (SAS) ve IFAC'ın hazırladığı Uluslararası Denetim Standartları (ISA), iç kontrolü COSO çerçevesine uygun olarak ele alır. SAS 109 İşletme ve Çevresinin Anlaşılması ve Önemli Yanlışlık Riskinin Değerlendirilmesi Standardı ve ISA 315 İşletme ve Çevresini Tanıyarak Önemli Yanlışlıkların Belirlenmesi Standardı, iç kontrolü COSO ile uyumlu olarak düzenlemiştir.

COSO Çerçevesi, iç kontrolü beş temel bileşene ayırmıştır. Bu bileşenlerin birbirleriyle ilişkisi ve birbirlerini nasıl etkilediklerinin anlaşılması, iç kontrolün anlaşılması açısından önemlidir. COSO, iç kontrol bileşenlerinin birbirleriyle sıkı bir ilişki içinde olduğunu savunur. Her bir bileşen diğeriyle ilişkilidir ve diğer bileşenin işleyişini etkiler. COSO iç kontrol bileşenleri aşağıda özlü bir şekilde açıklanmıştır (Graham, 2015, s.3; COSO, 2013, s.4-5). COSO iç kontrol bileşenleri Şekil 2.7'de gösterilmiştir.




**Şekil 2.7.** *COSO Küpü*

***Kontrol Ortamı***: Kontrol ortamı, diğer dört iç kontrol bileşenine temel oluşturur. İç kontrolün işletme içerisinde yürütülmesine temel oluşturan standartlar, süreçler ve yapılar

iç kontrol ortamını oluşturur. Kontrol ortamı, işletmenin iç kontrolünün tamamına nüfuz eden bir etkiye sahiptir. İşletmede etkin işleyen bir iç kontrol yapısının kurulabilmesinin ön koşulu, uygun bir kontrol ortamının oluşturulmasıdır. Üst yönetim, işletme çalışanlarının kontrol bilinciyle hareket etmesini, uygun politikalarla teşvik etmelidir. Yönetim kurulu, üst yönetim ve çalışanlar, işletme içinde iç kontrole yönelik destekleyici bir ortamın oluşturulması ve sürdürülmesi için çaba harcamalıdır. İşletmede kontrol ortamının temel bileşenleri şunlardır (Hall, 2011, s.17):

- Dürüstlük ve etik değerler;
- Örgütsel yapı;
- İşletmenin yönetim kurulu ve denetim komitesinin oluşumu;
- Yönetimin felsefesi ve çalışma tarzı;
- Yetki ve sorumlulukların dağıtılması amacıyla geliştirilen yordamlar;
- Yönetimin performans değerlendirme yöntemleri;
- Düzenleyici kurumların incelemeleri gibi dış etkenler;
- İşletmenin insan kaynakları politikaları ve yordamlarıdır.

***Risk Değerlendirme***: Bütün işletmeler iç ve dış kaynaklı çeşitli risklere maruz kalırlar. Risk değerlendirme, işletmenin amaçlarına ulaşılmasının önündeki riskleri belirlenmesi ve değerlendirilmesinden oluşan dinamik ve sürekli olarak tekrarlanan bir süreçtir. İşletmenin çeşitli seviyelerinde belirlenen risk yaklaşımına göre, amaçları etkileyen riskler kontrol altında tutulmalıdır. Risk değerlendirme, risklerin nasıl yönetileceğinin belirlenmesine bir temel oluşturur. İşletmenin çeşitli seviyelerinde amaçların belirlenmesi için bir önkoşuldur. Yönetim; faaliyet, raporlama ve uygunluk kategorilerindeki amaçları ve bu amaçlara ilişkin risk analizlerini ve değerlendirmeleri yeterli açıklıkla belirlemelidir. Ayrıca yönetim, amaçların uygunluğunu da dikkate almalıdır. Risk değerlendirme, yönetimin iç kontrolün etkinliğini sağlayan kendi işletme modelinde ve dış çevrede meydana gelebilecek değişimlerin etkisini dikkate almasını da gerektirir. Risk değerlendirme, riskleri saptamak ve incelemek, riskleri uygun seviyede tutacak kontrolleri oluşturmak ve değişen risklere göre iç kontrolün geliştirilmesini gerektirir.

***Kontrol Faaliyetleri***: Kontrol faaliyetleri, riskin azaltılması ve işletme amaçlarına ulaşılması amacıyla yönetimin direktiflerinin güvence altına alınmasına destek sağlayan politika ve yordamlardan oluşur. İşletmenin tamamını ve bütün birimlerini etkileyecek biçimde çeşitli işletme seviyelerinde bulunan işletme süreçlerinde ve işletmenin bilgi

teknolojileri ortamı üzerinde yürütülebilir. Kontrol faaliyetleri, önleyici veya ortaya çıkarıcı bir yapıda manuel veya otomatik faaliyetlerdir ve onaylamalar, yetkilendirmeler, doğrulamalar, mutabakatlar, işletme performansının incelenmesi ve görevlerin ayrılığı gibi çeşitli faaliyetlerden oluşur. Kontrol politikaları ve yordamları, satış ve harcama işlemleri gibi günlük işlemlerin veya işletme varlıklarının korunması gibi amaçlarla periyodik olarak yapılan işlemlerin sağlıklı bir şekilde yürütülmesini sağlamak amacıyla geliştirilmeli ve uygulanmalıdır. Belli başlı kontrol faaliyetleri şöyle sıralanabilir:

- Görevlerin ayrılması;
- İşlem ve süreçlere ilişkin yetkilendirmeler;
- Yeterli seviyede belgelendirme ve kaydetme;
- Varlıkların ve kayıtların fiziki kontrolü;
- İşlem ve süreçlerin bağımsız kişiler tarafından doğrulanması.

***Bilgi ve İletişim***: Bilgi, işletme içinde amaçlara ulaşılmasını destekleyen iç kontrol sorumluluklarının üstlenilmesi için gereklidir. Yönetim iç kontrolün diğer bileşenlerini desteklemek amacıyla iç ve dış kaynaklardan kaliteli ve ilgili bilgiyi elde eder, analizleriyle yeni bilgiler üretir ve gerektiğinde bu bilgilerden faydalanır. İletişim, ihtiyaç duyulan bilginin elde edilmesi ve paylaşılması için süreklilik gösteren bir süreçtir. İç kontroller ne kadar iyi tasarlansa da, bilgi ve iletişim bileşeni olmadan etkili olmaları beklenemez. İşletme içi iletişim, işletmenin tamamında yukarıdan aşağıya bilgi akışının sağlanması anlamına gelir. İşletme çalışanlarının yönetimin üstlenmeleri gereken kontrol sorumlulukları hakkındaki mesajını net bir şekilde almalarına olanak sağlar. Dış iletişim hem işletme dışından ilgili bilginin işletmeye aktarımını hem de işletme dışındaki tarafların beklentileri ve işletmenin uyması gereken düzenlemeler hakkındaki bilginin üçüncü taraflara aktarımını sağlar.

***İzleme***: COSO çerçevesi iç kontrolü bir yönetim sorumluluğu olarak tanımlar. İç kontrollerin geliştirildikleri durumlar zamanla değişebilir ve bir zamanlar etkin şekilde işleyen bir kontrol zamanla etkisini yitirebilir veya tamamen geçersiz hale gelebilir. İç kontrollerin gerektiği gibi çalışıp çalışmadığının yönetim tarafından sürekli olarak izlenmesi gerekir. İzlemenin temel amacı, iç kontrol sisteminin değişen koşullar karşısında hala etkin olarak çalışıp çalışmadığının değerlendirilmesidir. İzleme faaliyeti, sürekli değerlendirme ve özel değerlendirme veya bu ikisinin bir kombinasyonu olarak gerçekleştirilebilir. İç kontrol yapısı genellikle belli bir seviyeye kadar sürekli

değerlendirmeye uygun olarak geliştirilmelidir. Sürekli değerlendirmenin kapsamı ne kadar geniş tutulursa, özel değerlendirmelere o kadar az ihtiyaç duyulur.

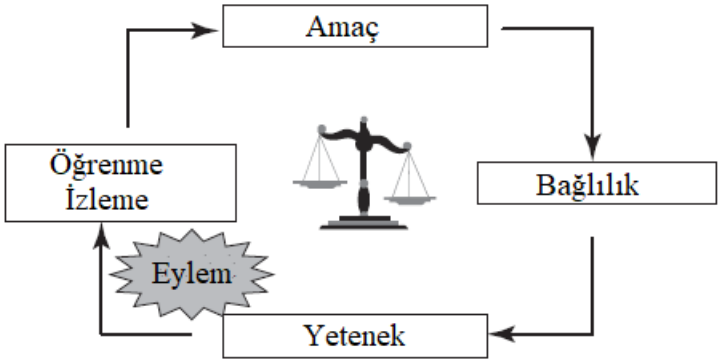
2013 yılında gözden geçirilerek yayımlanan güncel COSO Çerçevesinde, her bir iç kontrol bileşeninin etkinliğinin altında yatan temel kavramları yansıtan 17 ilke belirlenmiştir. İç kontrol bileşenlerini destekleyen bu 17 ilke, işletmenin faaliyet, raporlama ve uygunluk amaçları için uygulanmalıdır. İşletme içerisinde bu 17 ilke uygulanarak etkili bir iç kontrol yapısı geliştirebilir. Bu ilkeler Tablo 2.6'da yer almaktadır:

**Tablo 2.6.** *COSO İç Kontrol Bileşenlerini Esas Alan İlkeler (COSO, 2013, s. 6-7)*

| |
|---|
| ***Kontrol Ortamı*** |
| 1. İşletmenin yönetim kurulu, üst yönetimi ve bütün çalışanları dürüstlük ve etik değerlere bağlılık göstermelidir. |
| 2. Yönetim kurulu icradan bağımsız olmalı ve iç kontrolün geliştirilmesi ve performansını izlemelidir. |
| 3. Yönetim, yönetim kurulunun gözetiminde raporlama sistemini, örgütsel yapıyı ve amaçlara ulaşılması amacıyla uygun yetkilendirme ve sorumlulukları düzenlemelidir. |
| 4. Yönetim işletme amaçlarıyla tutarlı şekilde yetkin çalışanları işletmeye çekmeli, istihdam etmeli ve becerilerini geliştirmeleri için eğitilmelerini sağlamalıdır. |
| 5. İşletmede amaçlara uygun iç kontrol sorumlulukları hakkında çalışanların hesap verebilir olması sağlanmalıdır. |
| ***Risk Değerlendirme*** |
| 6. İşletme amaçları, ilişkili risklerin belirlenmesine ve değerlendirilmesine olanak sağlayacak açıklıkla belirlenmelidir. |
| 7. Risklerin nasıl yönetileceğini belirlemek amacıyla maruz kalınan riskler analiz edilmeli ve amaçlara ulaşılmasının önündeki riskler belirlenmelidir. |
| 8. İşletme amaçlarının önündeki riskler değerlendirilirken potansiyel hileler göz önünde bulundurulmalıdır. |
| 9. İç kontrol sistemi üzerinde önemli etkisi olabilecek değişiklikler belirlenmeli ve değerlendirilmelidir. |
| ***Kontrol Faaliyetleri*** |
| 10. Amaçlara ulaşılmasının önündeki riskleri kabul edilebilir bir seviyeye indirmeye katkı sağlayabilecek kontrol faaliyetleri seçilmeli ve geliştirilmelidir. |
| 11. Bilgi teknolojileri üzerinde işletme amaçlarını destekleyen genel kontrol faaliyetleri seçilmeli ve geliştirilmelidir. |
| 12. İşletme politikalarına, kontrol faaliyetleri ve politikalara uygun yordamlar uygulanmalıdır. |
| ***Bilgi ve İletişim*** |
| 13. İç kontrol bileşenlerini desteklemek amacıyla ilgili ve kaliteli bilgi elde edilmeli, üretilmeli ve kullanılmalıdır. |
| 14. İç kontrol fonksiyonlarını desteklemek için gerekli olan iç kontrol sorumluluklarına ve amaçlarına ilişkin bilgi, işletme içinde ilgili taraflara iletilmelidir. |
| 15. İç kontrol fonksiyonunu etkileyen ilgili hususlar üçüncü taraflara iletilmelidir. |
| ***İzleme*** |
| 16. İç kontrol bileşenlerinin varlığını ve işlerliğini belirlemek amacıyla sürekli ve/veya özel değerlendirmeler seçilmeli, geliştirilmeli ve yürütülmelidir. |
| 17. İç kontrol eksiklikleri değerlendirilmeli ve düzeltici önlemler almaktan sorumlu olan yönetim kurulu, üst yönetim ve çalışanlar gibi taraflara zamanında iletilmelidir. |

### *2.16.6.2. CoCo çerçevesi*

Denetim ve muhasebe alanında Kanada'daki mesleki örgüt olan Kanada Sertifikalı Muhasebeciler Enstitüsü (The Canadian Institute of Chartered Accountants - CICA), 1995 yılında kontrol sistemlerinin tasarlanması, değerlendirilmesi ve raporlanması konusunda işletmelere yol göstermek için bir rehber hazırlanması amacıyla bir çalışma grubu kurmuştur. Çalışma grubu, amaçları doğrultusunda Kontrol Ölçütleri (Criteria of Control – CoCo) adıyla bir çerçeve hazırlamıştır. CoCo'ya göre kontrol, işletmenin amaçlarına ulaşılmasında çalışanlara destek sağlayan kaynaklar, sistemler, süreçler, kültür, yapı ve görevlerden meydana gelir. COSO ile karşılaştırıldığında biraz farklılık gösterir. CoCo Çerçevesinde iç kontrol; amaç, bağlılık, yetenek, izleme ve öğrenme bileşenlerinden oluşur. CoCo Çerçevesi, COSO Çerçevesiyle tutarlıdır ama COSO'ya göre anlaşılması daha kolay bir iç kontrol modeli sağlar (Moeller, 2004, s.267). CoCo bileşenleri aşağıda kısaca açıklanmıştır (Pickett, 2011, s.109). Şekil 2.8'de CoCo iç kontrol çerçevesinin unsurları gösterilmiştir.




**Şekil 2.8.** *CoCo Çerçevesi Unsurları (Pickett, 2011, s. 110)*

***Amaç***: CoCo iç kontrol modeline göre, çalışanların açık şekilde yönlendirilmesini sağlayan bir amaç duygusunun geliştirilmesi gerekir. Bu kapsamda amaçlar, vizyon, misyon, strateji, riskler ve fırsatlar, politikalar, planlar, performans amaçları ve göstergeleri açıkça belirlenmelidir. Çalışanların kurumsal amaçlar doğrultusunda görevlerini yerine getirmesi, amaçlara ulaşılması için kontrollerin geliştirilmesi ve kontrol ölçütlerinin belirlenmesi amacıyla açık bir yönlendirmeye sahip olunması işletmeler için olmazsa olmazdır.

***Bağlılık***: İşletme içinde çalışanların işletmenin kimliğini ve değerlerini anlaması ve uyum göstermesi gereklidir. Bu kapsamda etik değerler, dürüstlük, insan kaynakları politikaları yetkilendirme, sorumluluklar ve hesap verebilirlik ve karşılıklı güven geliştirilmelidir. Kontrol sisteminde görülen birçok başarısızlık, işleyişin doğal bir parçası olan kontrol ahlakına işletme çalışanlarının bağlılığının olmayışından kaynaklanır.

***Yetenek***: Çalışanlar, kontrol modelinin gerekliliklerini anlayabilecek ve yerine getirebilecek kaynaklara ve yeteneklere sahip olmalıdır. Bu kapsamda bilgi, yetenek ve araçlar, iletişim süreçleri, bilgi koordinasyonu ve kontrol faaliyetleri geliştirilmelidir. Herkes açıkça belirlenen amaçlar ile uyumlu iyi kontrollerin tasarımı ve geliştirilmesine katılmak amacıyla hazır durumda olmalıdır ve örgütsel yaşam açısından gerekli olan uzmanlık geliştirilmelidir.

***İzleme ve öğrenme***: Çalışanlar işletmenin gelişiminin bir parçasıdır. Bu kapsamda iç ve dış çevre izlenmeli, bilgi ihtiyacı ve bilgi sistemleri yeniden değerlendirilmeli, performans izlenmeli, kontrol yordamları ve kontrollerin etkinliği değerlendirilmelidir. İzleme süreci inceleme, kontrol ve danışmanlık faaliyetleriyle uyumlu olmalıdır. Ayrıca çalışanların gelişiminin sağlanması da önemli bir kontroldür. İşletme, suçlama kültürüyle pozitif öğrenme deneyimlerini destekleyemez. Böyle işletmelerde kontroller - çok yanlış biçimde- düşük performanslı çalışanları cezalandırma mekanizması olarak görülecektir. CoCo ölçütlerine göre kontroller uygun geri besleme süreçlerini desteklemelidir.

CoCo Çerçevesi, dört bileşenin geliştirilmesi amacıyla, denetim süreçlerinde de yararlanılabilecek 20 iç kontrol ilkesi belirlemiştir. Bu ilkeler Tablo 2.7'de yer almaktadır:

**Tablo 2.7.** *CoCo Çerçevesi İlkeleri (Sawyer, Dittenhofer, Scheiner, 2005, s. 68-69)*

***Amaç***

1. Amaçlar belirlenmeli ve işletme çalışanlarına iletilmelidir.
2. Amaçlara ulaşılması karşısında işletmenin maruz kaldığı önemli iç ve dış riskler belirlenmeli ve değerlendirilmelidir.
3. Yönetim tarafından amaçlara ulaşılmasını desteklemek için politikalar geliştirilmeli ve özgürce hareket edebilecekleri sınırları ve kendilerinden beklenenleri anlamaları amacıyla çalışanlara iletilmelidir.
4. Amaçlar doğrultusunda planlar geliştirilmeli ve çalışanlarla paylaşılmalıdır.
5. Amaçlar ve ilgili planlar ölçülebilir performans göstergelerini kapsamalıdır.

***Bağlılık***

6. İşletme içinde dürüstlük ve etik değerlerin paylaşılması ve iş süreçlerinde bu doğrultuda hareket edilmesi sağlanmalıdır.
7. İnsan kaynakları politika ve yordamları, işletmenin etik değerleri ve amaçlarıyla tutarlı olmalıdır.
8. Yetki, sorumluluk ve hesap verebilirlik açıkça belirlenmeli ve işletme amaçlarıyla tutarlı olmalıdır, böylece karar alma ve eylemler uygun çalışanlar tarafından yapılabilir.
9. Çalışanlar arasında bilgi akışını destekleyen ve onların amaçlar doğrultusunda etkin performans göstermesini sağlayan karşılıklı güven atmosferi tesis edilmelidir.

***Yetenek***

10. Çalışanlar işletme amaçları doğrultusunda gerekli olan bilgi ve beceriye sahip olmalıdır.
11. İletişim süreçleri işletmenin değerleri ve amaçlarını desteklemelidir.
12. Çalışanların sorumluluklarını üstlenebilmeleri için yeterli ve ilgili seviyede bilgi belirlenmeli ve zamanında onlara iletilmelidir.
13. İşletmenin farklı bölümlerindeki karar alma süreçleri ve faaliyetler arasında koordinasyon sağlanmalıdır.
14. Kontrol faaliyetleri amaçlar, riskler ve kontrol bileşenleri arasındaki ilişkiyi hesaba katacak şekilde işletmenin ayrılmaz bir parçası olarak tasarlanmalıdır.

***İzleme ve Öğrenme***

15. İç ve dış çevre, işletmenin amaçlarının ve kontrollerinin yeniden değerlendirilmesi ihtiyacının ortaya çıktığına ilişkin bir sinyal elde etmek amacıyla sürekli olarak izlenmelidir.
16. Performans, işletme amaçları ve planlarında belirlenen göstergelere göre sürekli olarak izlenmelidir.
17. İşletmenin amaçları ve sistemlerinin arkasındaki varsayımlar düzenli olarak test edilmelidir.
18. Bilgi ihtiyacı ve ilgili bilgi sistemleri değişen amaçlar veya belirlenen raporlama eksikliklerine göre yeniden değerlendirilmelidir.
19. Kullanılan yordamlar uygun değişime veya ortaya çıkan eylemlere cevap verebilmek amacıyla geliştirilmeli ve yürütülmelidir.
20. Yönetim, kontrollerin etkinliğini düzenli olarak gözden geçirmeli ve sonuçları hesap vermekten sorumlu olan çalışanlar ile paylaşmalıdır.

### *2.16.6.3. Bilgi ve ilgili teknolojiler için kontrol amaçları (Control objectives for information and related technology – COBIT)*

COBIT Çerçevesi; bilgi sistemleri denetimi ve kontrolleri hakkında çalışmalar yapan bağımsız ve kar amacı gütmeyen bir kuruluş olan Bilgi Sistemleri Denetim ve Kontrol Birliği (Information Systems Audit and Control Association – ISACA) ve kurumsal başarı için bilgi teknolojileri alanında yönetim kurulları ve işletme yöneticilerine destek olmayı amaçlayan bir kuruluş olan Bilgi Teknolojileri Yönetişim Enstitüsü (Information Technology Governance Institute – ITGI) tarafından geliştirilmiştir. 1996 yılında ilk defa yayınlanan COBIT Çerçevesi, ihtiyaçlar doğrultusunda yeniden düzenlenmiştir. 2012 yılında COBIT 5.0 adıyla son versiyonu yayımlanmıştır. COBIT, bilgi teknolojileri denetimi ve BT ortamında kontrollerin geliştirilmesi amacıyla rehberlik sağlar. Ayrıca BT yönetişimi için yöneticilerin kullanımına uygun bir çerçevedir.[3]

Bankacılık Düzenleme ve Denetleme Kurumunun (BDDK) 2006 yılında ülkemizdeki bankaları COBIT Çerçevesini esas alan bir yaklaşımla denetime alması, COBIT'in ülkemiz kamuoyunda bilinirliğini artırmıştır. COBIT'in BDDK tebliğlerinde kendisine yer bulması ülkemiz açısından öneminin artmasına, yaygınlaşmasına ve bankalar dışındaki işletmelerin de dikkatini çekmesine yol açmıştır (Güneş vd., 2013, s.5).

COBIT'in misyonu; işletme yöneticileri ve denetçiler tarafından kullanılması amacıyla yeterli, geçerli, modern ve uluslararası kabul görmüş BT kontrol amaçlarını sürekli olarak araştırmak, geliştirmek ve uygulanmasını sağlamaktır (Uzunay, 2007, s.5). COBIT Çerçevesi, İşletmenin tamamında BT kontrolünü sağlamak için şeffaf politikalar geliştirilmesini ve başarıyla uygulanmasını sağlar. COBIT kontrol çerçevesi, bilgi teknolojilerinin işletmenin ihtiyaçlarını yerine getirebilmesi amacını taşıyan bir iç kontrol modelidir. BT faaliyetlerini genel kabul görmüş bir süreç modeli şeklinde örgütler. BT kaynaklarını tanımlar ve işletmenin kontrol amaçlarını açıklar.

COBIT ilk olarak bir denetim aracı olarak tasarlanmasına karşın, bilgi işleme ve işletme yönetiminde kullanılan bir araç haline gelmiştir. İşletmenin iş hedefleri doğrultusunda hizmet vermesini sağlamak amacıyla, bilgi işlem kaynaklarını kullanmasını amaçlar ve verilen hizmetlerin, istenilen kalite, güvenlik ve hukuki

[3] COBIT hakkında ayrıntılı bilgi için bakınız: https://www.isaca.org/COBIT/Documents/An-Introduction.pdf

ihtiyaçlara cevap verebilmesini sağlar. Yönetimin kontrol gereksinimleri, teknik konular ve riskler arasında köprü kurmasına yardımcı olan bir yönetişim çatısıdır.

COBIT bilgi teknolojileri kontrollerinin ve risklerinin yönetilmesine olanak tanır. Kontroller üzerinde yüksek seviyede güvenilirlik sağlayan 34 BT sürecinden ve 318 detaylı kontrol amacı ve denetim rehberinden oluşur. Bu süreçler dört alanda gruplandırılmıştır: planlama ve organizasyon, kurulum ve uygulama, işlerlik kazandırma ve destekleme, izleme. Bu yapı, desteklenen bilgi ve teknolojilerin bütün yönlerini kapsar. Yönetimin ihtiyaç duyduğu uygun seviyede BT güvenliği ve kontrollerinin belirlenmesi ve izlenmesine destek sunan iyi güvenlik ve kontrol pratiklerinden oluşan uygulanabilir ve genel kabul görmüş standartlardan oluşur (Soltani, 2007, s.421). COBIT, süreçlerini kısaca şöyle tanımlamıştır (Moeller, 2008, s.126):

***Planlama ve Organizasyon***: İşletmenin kurumsal amaçlarını en iyi şekilde destekleyen ve katkıda bulunan BT stratejileri ve taktikleri geliştirilmelidir. Bu kapsamda işletmenin stratejik BT vizyonu bütün işletmeyle paylaşılmalı, işletmenin misyonunu bu yönde yönlendirmeli ve BT'nin işletme içinde bütün taraflar için gerçekleştirilmeye çalışılan çabalar olduğu vurgulanmalıdır.

***Kurulum ve Uygulama***: BT çözümlerinin belirlenmesi, geliştirilmesi veya kurulması gereklidir ve BT'nin iş süreçlerine uygunluğu sağlanmalıdır. Bu alan, var olan sistemlerin değişimini ve bakımını düzenler.

***İşlerlik kazandırma ve Destekleme***: Uygulama ve altyapı araçlarından oluşan hizmetlerin BT süreçlerinin işlerlik kazanması ve desteklenmesi bu alanın kapsamındadır. Uygulama ve kontrollerin fiili olarak işlerlik kazandığı alandır.

***İzleme***: BT kontrol süreçlerinin kalite ve uygunluğunun izlenmesi ile bağımsız denetim ve iç denetim süreçlerinin değerlendirilmesinden oluşur.

COBIT'in işletme yönetimine, BT personeline, bağımsız ve iç denetçilere, işletme içi ve işletme dışı bilgi kullanıcılarına sayısız faydaları vardır. İç denetçilere sağladığı faydalar şöyle sıralanabilir (Pekel, 2008, s.18):

- Denetçiler, denetim konularında yaşanabilecek kapsam ve objektif ölçüt belirleme sorunlarını COBIT ile aşabilirler. Çünkü COBIT çok sayıda uzman görüşüyle hazırlanmış ve var olan tüm ölçütler dikkate alınarak hazırlanmış bir çerçevedir.
- Denetçiler, denetim rehberinden faydalanarak, belirlenen risklerin doğurabileceği zararları somutlaştırabilirler ve böylece yönetime riskler ve iç kontrollere ilişkin daha sağlıklı raporlar sunabilirler.

- Denetçiler, COBIT'in sunduğu kritik başarı faktörlerinden yararlanılarak denetim sonuçlarını ölçümleyebilir ve daha sağlıklı iyileştirme önerileri getirebilirler.
- BT'leri personelinin BT denetiminin hangi ölçütlere göre yapıldığını bilmesi, denetimin daha verimli yapılmasını ve geliştirilmesi gereken alanların daha kolay farkına varılmasını sağlayabilir.

#### *2.16.6.4. Bilgi teknolojileri altyapı kütüphanesi (Information technology infrastructure library – ITIL)*

Bilgi Teknolojileri Altyapı Kütüphanesi, İngiltere Ticaret Bakanlığı Bilgisayar ve Telekomünikasyon Kurumu tarafından, bilgi teknolojilerine olan artan bağımlılık sonucunda ortaya çıkan ihtiyaçların daha etkin şekilde giderilmesi amacıyla tavsiyeler seti olarak ilk defa 1987 yılında yayımlanmıştır. ITIL, her biri spesifik BT hizmet yönetimi hakkındaki kitapların bir araya getirilmesiyle oluşturulmuştur. ITIL'ın amacı, BT hizmetlerinin işletmenin iş süreçlerine uygun olarak düzenlenmesi ve iş süreçlerine ilişkin ihtiyaçların giderilmesidir. ITIL, iş değişikliklerinin ve büyümenin kolaylaştırılabilmesi için BT'den nasıl faydalanılabileceği konusunda işletmelere rehberlik sağlar. İşletme faaliyetlerinde kullanılan yordam, görev ve kontrolleri tanımlar. İşletmenin planlayabileceği, uygulayabileceği ve ölçümleyebileceği bir temel oluşturmasına olanak sağlar. İş süreçlerinin BT ile uyumu ve gelişimi için kullanılır (Bağcı, 2014, s.348).

ITIL, bütün işletmelerde ve işletme ortamlarında uygulanabilen ve adaptasyon gösteren BT hizmetlerini belirleme, planlama, sunma ve destekleme amacına yönelik güçlü bir çerçevedir. Bütün dünyada BT hizmet yönetimi amacıyla en yaygın kullanılan yaklaşımlardan biridir. BT kullanımında işletmedeki değişimin, dönüşümün ve büyümenin farkında olmaları için işletmelere ve çalışanlara destek sunar. İşletme riski ve hizmet kesintilerinin yönetilmesi, özellikle müşteri ve tedarikçiler gibi işletme paydaşlarıyla ilişkilerin geliştirilmesi, işletmede ihtiyaç duyulan maliyet etkin sistemlerin geliştirilmesi ve istikrarlı bir işletme ortamı sağlanması için iş değişiminin desteklenmesi en temel faydalarıdır.[4]

Temel olarak bir hizmet yönetimi yaklaşımı olan ITIL, BT hizmetleriyle iş ihtiyaçları arasındaki uyumun sağlanmasını amaçlar ve uyum seviyesini BT kalitesi

[4] Ayrıntılı bilgi için bakınız: https://www.axelos.com/best-practice-solutions/itil

olarak tanımlar. Bilgi teknolojileri süreçlerine odaklanıp, süreç geliştirme aşamasında nelerin dikkate alınması gerektiğini açıklar ve işletmenin iş süreçlerinin BT'ye yansıtılmasını sağlar (Taşçı & Yılmaz, 2011, s.3).

İç denetim perspektifinden bakıldığında ITIL'ın sunduğu BT ortamında en iyi uygulamalar seti, iç denetçinin BT iç kontrol risklerini incelemesi ve etkili BT kontrollerini geliştirmesi amacıyla kullanabileceği bir rehberdir. ITIL, işletmenin BT altyapısını kurmasında ve işletme süreçlerini BT ortamında yürütebilmesinde yol gösterir. İç denetçi, hem işletme süreçlerini iyi anlamalı hem de uygun kontrolleri geliştirmelidir. ITIL'ın en iyi uygulamalar seti, süreçlerin BT ortamında etkili işletilmesinin yanında bu süreçlere iyi tasarlanmış kontroller yerleştirilmesinde de rehberlik eder.

ITIL, sadece iç kontrolün geliştirilmesine yönelik bir çerçeve olarak hazırlanmamıştır, işletmenin BT yönetişimi, iş süreçlerinin BT ile uyumu ve BT güvenliği ve kontrollerinin geliştirilmesini sağlayan tavsiyelerden oluşur. İşletme kontrolleri ve denetim sürecinin sürekli geliştirilmesi uygulamalarının, BT'leri ortamında etkin bir şekilde yerine getirilmesini sağlayan kontrol listeleri ve doküman şablonları sunar. Kapasite yönetimi, gereksinim yönetimi, talep yönetimi, erişilebilirlik, bilgi güvenliği, tedarikçi yönetimi gibi süreçlerde yönetime BT ortamında etkin işleyen kontroller geliştirmesi için yol gösterir. İç denetçilere ve yönetime bilgi teknolojilerini yönetme ve işletmeye değer sağlama, BT hizmetlerini ve iş süreçlerini ölçme, izleme ve optimize etme, BT'ye uygun standartları tanımlama ve hesap verebilir bir BT yapısı inşa etme amaçlarına ulaşılması için yardımcı olur (Bağcı, 2014, s.349-350).

#### *2.16.6.5. Turnbull raporu modeli*

İngiltere'de halka açık işletmelerin, Birleşik Kodda yer alan iç kontrole ilişkin gereklilikleri yerine getirmesinde rehberlik sağlayan 'İç Kontrol: Birleşik Kod Hakkında Yöneticiler için Rehber' isimli rapor, ilerleyen yıllarda raporu hazırlayan komitenin başkanı olan Nigel Turnbull'un adıyla anılmıştır. Rapor 1999 yılında İngiltere ve Galler Sertifikalı Muhasebeciler Enstitüsü (Institute of Chartered Accountants in England & Wales) tarafından yayımlanmış ve Ekim 2005'te Finansal Raporlama Konseyi (Financial Reporting Council - FRC) tarafından güncellenmiştir. Rapor özü itibariyle, yönetim kurulunun iç kontrol hakkında uygun politikaları geliştirmesinin ve risklerin yönetilmesinde iç kontrol sisteminin yönetim kurulunun onayladığı gibi ve etkin bir

biçimde çalıştığına dair makul güvence sağlanması gerektiğinin altını çizer (Hayes vd., 2005, s.66).

Rapor işletmenin yönetim kurulunun risk bazlı bir yaklaşımla güçlü iç kontrolü kurmasını ve etkinliğinin incelenmesini benimseyen bir temelde geliştirilmiştir. Bu anlayış işletmenin yönetimi ve yönetişim süreçleri içine dahil edilmelidir. Rapor amaçlarını şöyle sıralamıştır (Financial Reporting Council, 2005, s.3-4):

- İç kontrolün işletme amaçlarına ulaşılması için yürütülen iş süreçlerine yerleştirilmesini sağlayan güçlü işletme uygulamalarını yansıtmak;
- Sürekli değişen işletme ortamında geliştirilen ilkeler ile geçen zamana karşın uyumlu kalabilmek;
- Her işletmenin özel koşullarını hesaba katarak, raporun her işletmede uygulanabilmesini sağlamaktır.

İlk yayımlandığı 1999 yılından güncellendiği 2005 yılına kadar, rapordan faydalanan işletmelerin yönetim kurulları ve yatırımcılarından alınan değerlendirmelere göre, işletmelerinin iç kontrol ve risk yönetimi yapılarını raporda belirlenen ilkeleri dikkate alarak geliştiren işletmeler büyük yararlar sağlamıştır. Geri bildirimde bulunan kullanıcılara göre, raporun ilke bazlı olması ve COSO'nun aksine uygulama rehberi içermemesi bir sorun olmamıştır. Aksine bu durum, yönetim kurullarının işletmelerinin içinde bulunduğu özel koşulları göz önünde bulundurarak, iç kontrole ilişkin uygun hamleleri yapmaları konusunda avantajlı bir konumda olmalarını sağlamıştır (Türedi vd., 2015, s.109).

2005 yılında güncellenen haliyle rapor beş bölümden oluşur. Giriş bölümünde, iç kontrol ve risk yönetiminin önemi, raporun amaçları, Birleşik Koddaki iç kontrol gereklilikleri açıklanmıştır. İkinci bölümde güçlü bir iç kontrolün bileşenleri ve iç kontrol sorumlulukları; üçüncü bölümde iç kontrolün etkinliğinin incelenmesi süreci ve sorumluluklar; dördüncü bölümde iç kontrole ilişkin yönetim kurulu açıklamaları konularına yer verilmiştir. Son bölümde ise, işletmenin risk ve kontrol süreçlerinin etkinliğinin değerlendirilmesi için iç kontrol bileşenleri temelinde ayrımlanmış olarak ölçütler yer alır. Raporda iç kontrol bileşenleri COSO'ya uygundur, ancak ilk bileşen olarak risk değerlendirme ele alınmıştır. Bu durum, raporun daha çok risk değerlendirme odaklı olduğunu gösterir.

### *2.16.6.6. Basel komitesi modeli*

Basel Komitesinin sekretaryasını Uluslararası Ödemeler Bankası (Bank for International Settlements – BIS) yapar. Uluslararası finansal işbirliğini ve stabiliteyi geliştirme, ekonomik araştırmalarda merkez olma ve ulusal merkez bankaları için bir kredi ve ödeme bankası olma fonksiyonlarını üstlenmek üzere İsviçre'nin Basel kentinde 1930'da kurulan BIS, dünyanın en eski uluslararası finans kuruluşudur. Basel Komitesi ise, 1974 yılında birçok gelişmiş ülkenin (Belçika, Kanada, Fransa, Almanya, İtalya, Japonya, Lüksemburg, Hollanda, İsveç, İsviçre, İngiltere, ABD) merkez bankası başkanlarının katılımıyla kurulmuştur. Komite uluslararası bankacılık sisteminin güçlendirilmesi ve güvenilirliğinin artırılması amacıyla özellikle sermaye oranları ve likidite riski gibi konularda kararların alındığı ve denetim problemlerinin tartışıldığı bir forum niteliğindedir (Yavuz, 2002, s.55-56).

Basel Komitesine göre etkin işleyen bir iç kontrol, banka yönetiminin en önemli bileşenlerinden biridir ve banka organizasyonunun güvenli ve sağlam çalışmasının temelini oluşturur. COSO iç kontrol çerçevesini benimseyen komite, iç kontrolü COSO'nun beş ana başlığı altında değerlendirir. Ancak komitenin kararları ve yayınları yine de özellikle bankalar ve finansal hizmetler sektörü için iç kontrol alanında önemli bir tavsiye kaynağıdır (Pickett, 2010, s.269). Komite, iç kontrolü oluşturan bileşenleri COSO'yla benzer şekilde tanımlamıştır (İbiş & Çatıkkaş, 2012, s.111):

- Yönetimin gözetimi ve kontrol kültürü;
- Riskin tanımlanması ve değerlendirilmesi;
- Kontrol faaliyetleri ve görevlerin ayrımı;
- Bilgi ve iletişim;
- Faaliyetlerin sürekli izlenmesi ve kusurların düzeltilmesidir.

Basel Komitesi iç kontrolün değerlendirilmesine ilişkin bir dizi ilke geliştirmiştir. Komitenin iç kontrol alanında yayımladığı en önemli belge, 1998 yılında yayımlanan Bankalarda İç Kontrol Sistemleri için Çerçeve (Framework for Internal Control Systems in Banking Organisations) adlı çalışmadır. Bu çerçevede;

- Etkili iç kontrolün bankanın sağlıklı bir şekilde yönetilmesinde en önemli bileşenlerden biri olduğu;
- İç kontrollerin bankaların ve finansal sistemin güvenilirliğinin temeli olduğu;

- Her bankanın kendi yapısı ve faaliyetlerinin niteliği, karmaşıklığı ve risk yapısıyla uyumlu bir iç kontrol modeli geliştirmesi gerektiği belirtilmiştir (Yavuz, 2002, s.40).

Basel Komitesi, çeşitli ülkelerde yaşanan tecrübelerin bir araya getirilmesiyle hazırladığı söz konusu raporunda iç kontrol kavramı, iç kontrolün amaçları ve iç kontrolün birbiriyle ilişkili beş temel bileşeni hakkında yaptığı değerlendirmelerinin yanı sıra iç kontrolün değerlendirilmesine ilişkin 13 temel ilkesini belirlemiştir. Belgenin birinci bölümünde komitenin çalışmaları hakkında ön bilgi verilirken; ikinci bölümde bankalarda iç kontrolün önemi ve amaçlarına; üçüncü bölümde iç kontrol bileşenlerine yer verilmiştir. Dördüncü bölümde banka gözetim ve denetim otoritesinin iç kontrolün değerlendirmesinde yararlanacağı 13 ilke açıklanmış ve son bölümde iç kontrole ilişkin denetçi sorumlulukları belirlenmiştir (Yurtsever, 2008, s.37). Bu ilkeler Tablo 2.8'de kısaca açıklanmıştır.

**Tablo 2.8.** *Basel İç Kontrol Çerçevesi (Basle Committee on Banking Supervision, 1998, s. 2-3)*

***Yönetimin gözetimi ve kontrol kültürü***

1. Yönetim kurulu, bankanın genel işletme stratejisi ve önemli politikaların incelenmesi ve düzenli aralıklarla onaylanmasından; bankanın maruz kaldığı temel riskleri anlamak, riskleri kabul edilebilir seviyelere indirmek ve yönetimin riskleri tanımlaması, ölçmesi, izlemesi ve kontrol etmesi için gereken adımları atmasını sağlamak; örgütsel yapıyı onaylamak ve yönetimin iç kontrolün etkinliğini izlemesini sağlamaktan sorumludur. Yeterli ve etkin iç kontrol sistemlerinin kurulmasından ve işletilmesinden nihai olarak yönetim kurulu sorumludur.
2. Üst yönetim, yönetim kurulu tarafından onaylanan strateji ve politikaların uygulanmasından; bankanın maruz kaldığı risklerin belirlenmesi, ölçülmesi, izlenmesi ve kontrol altına alınması süreçlerinin geliştirilmesinden; yetki sorumluluk ve raporlama ilişkilerinin açıkça belirlendiği örgütsel yapının oluşturulmasından; devredilen sorumlulukların etkili bir şekilde üstlenilmesinden; uygun iç kontrol politikalarının geliştirilmesinden ve iç kontrolün yeterlilik ve etkinliğinin izlenmesinden sorumludur.
3. Yönetim kurulu ve üst yönetim doğruluğun ve etik standartların teşvik edilmesinden ve bütün seviyelerdeki çalışanlara iç kontrolün önemini gösteren ve vurgulayan işletme içi kültürün oluşturulmasından sorumludur. Bankadaki bütün çalışanlar, iç kontrol sürecindeki sorumluluklarını anlamalı ve süreçlere katılmalıdır.

***Riskin tanımlanması ve değerlendirilmesi***

4. Etkin bir iç kontrol, bankanın amaçlarına ulaşmasını önleyen önemli risklerin belirlenmesi ve değerlendirilmesini gerektirir. Bu değerlendirme bankanın karşılaşabileceği ve banka organizasyonuyla ilişkili bütün riskleri (kredi riski, ülke riski, transfer riski, piyasa riski, faiz oranı riski, likidite riski, operasyonel risk, yasal risk ve itibar riski) kapsar. İç kontrollerin, kontrol edilmeyen mevcut ve yeni riskleri kontrol altına alabilmek amacıyla gözden geçirilmesi gerekir.

**Tablo 2.8. (Devamı)** *Basel İç Kontrol Çerçevesi (Basle Committee on Banking Supervision, 1998, s. 2-3)*

***Kontrol faaliyetleri ve görevlerin ayrımı***

1. Kontrol faaliyetleri bankanın günlük işlemlerinin ayrılmaz bir parçası olmalıdır. Etkin işleyen bir iç kontrol, bütün işletme seviyelerinde tanımlanan kontrol faaliyetleriyle uyumlu kontrol yapısının kurulmasını gerektirir. Bu kapsamda üst yönetim incelemeleri; farklı birimler ve bölümler için uygun faaliyet kontrolleri; fiziksel kontroller; uygunsuzlukların takip edilmesi ve uygunluk sınırlarının aşılıp aşılmadığının kontrolü; yetki ve onay sistemi; doğrulama ve mutabakat sistemi bulunmalıdır.
2. Etkili iç kontrol, çalışanların sorumluluklarının çakışmamasını ve görevlerin uygun şekilde ayrılmasını gerektirir. Potansiyel çıkar çatışmaları belirlenmeli, azaltılmalı ve bağımsız biçimde izlenmelidir.

***Bilgi ve İletişim***

3. Etkili iç kontrol, bankanın yeterli ve kapsamlı finansal, operasyonel ve uygunluk verisinin yanı sıra dış çevrede bankanın karar alma süreciyle ilişkili olaylar ve durumlar hakkındaki bilginin de elde edilmesini gerekli kılar.
4. Etkili iç kontrol, bankanın bütün önemli faaliyetlerini kapsayan bilgi sistemlerinin güvenilirliğini gerektirir. Bu sistemler elektronik biçimde bilginin kaydedilmesi ve kullanılmasını sağlamalı, güvenilir olmalı, bağımsız olarak izlenmeli ve yeterli düzenlemelerle desteklenmelidir.
5. Etkili iç kontrol, uygun çalışanların ilgili bilgiye ulaşmasını ve bütün çalışanların görev ve sorumluluklarını etkileyen politika ve yordamları tam olarak anlamasını ve bağlı olmasını sağlayan etkili iletişim kanallarını gerektirir.

***Faaliyetlerin sürekli izlenmesi ve kusurların düzeltilmesi***

6. Bankanın iç kontrolünün etkinliği sürekli devam eden bir temelde izlenmelidir. Anahtar risklerin izlenmesi bankanın günlük faaliyetlerinin bir parçası olmalıdır ve iç denetim tarafından düzenli aralıklarla değerlendirilmelidir.
7. İç kontrolün operasyonel olarak bağımsız, uygun eğitimlere ve uzmanlığa sahip çalışanlar tarafından yürütülen etkili ve kapsamlı bir iç denetime sahip olması gerekir. İç kontrol sisteminin izlenmesinin bir parçası olarak iç denetim fonksiyonu doğrudan yönetim kuruluna, denetim komitesine ve üst yönetime raporlama yapmalıdır.
8. İşletme birimleri, iç denetim veya diğer kontrol çalışanları tarafından tespit edilen iç kontrol kusurları, uygun seviyedeki yöneticilere zamanında raporlanmalı ve derhal giderilmelidir. Önemli iç kontrol kusurları üst yönetime ve yönetim kuruluna raporlanmalıdır.

***İç kontrol sisteminin denetim ve gözetim otoritelerince değerlendirilmesi***

9. Bankanın gözetim ve denetim otoritesi, büyüklüğüne bakılmaksızın bütün bankaların, bankanın çevresindeki ve şartlarındaki değişime cevap verebilen ve bilanço ve bilanço dışı faaliyetlerindeki yapı, karmaşıklık ve risk yaklaşımıyla tutarlı etkili bir iç kontrole sahip olmasını istemelidir. Bankanın iç kontrolünün bankanın risk profili açısından yeterli ve etkili olup olmadığını tespit etmeli ve gerekli düzenleyici önlemleri almalıdır.

## 3. YRU (YÖNETİŞİM-RİSK YÖNETİMİ-UYGUNLUK) YAKLAŞIMI

Adam Smith, Ulusların Zenginliği kitabında ortaya attığı görünmez el metaforuyla, bireylerin kendi menfaatlerini düşünerek geliştirdikleri davranış biçimlerinin toplumun menfaatlerine de olumlu yönde katkı sağlayacağını, bu yüzden bireyin ve toplumun çıkarları arasında bir nedensellik olduğunu savunur. Buna göre kendi çıkarlarının peşinden koşan bireyler ve bu kapsamı genişletmek gerekirse sadece kendi menfaatleri için çalışan işletmeler, farkında olarak ya da olmayarak toplumun menfaatleri için de katkıda bulunmuş olurlar. Smith'in doktrini, doğal düzenin bireysel menfaatlere göre oluşacağı inancını taşıdığı için oportünist ve realisttir. Smith ile beraber ortaya çıkan fikirler, liberalizmin ve kapitalizmin de temel dayanağı olmuştur. Bu anlayışı savunanlar, devletin ekonomik düzene yasalar veya diğer düzenlemeler aracılığıyla sınırlar koymasına karşı çıkarlar. Bu anlayışa göre ekonomiye hükümet müdahaleleri, 'bırakınız yapsınlar' ilkesi gereğince minimum seviyeye indirilmelidir. Bu seviyede ancak sosyal devlet ilkesine bağlı olarak, örneğin fakirlere verilen yardımlar şeklinde tezahür edebilir.

Smith'in 18. yüzyılda ortaya attığı ve takipçileri tarafından 19. yüzyılda geliştirilen fikirler, 1929 büyük buhran döneminde tüm çevrelerden yoğun eleştiriler almaya başlamıştır. Bu eleştirilerin iki temel dayanağı vardır. Bunlardan ilkine göre, bireylerin ve daha geniş bir perspektifle bakıldığında işletmelerin kendi menfaatlerinin peşine düşmesi, hem liberalizmin hem de kapitalizmin savunduğu serbest piyasa kavramı ve hükümetler tarafından sınırlamalar getirilmeyen bir ekonomik ortamla birlikte, artan sanayileşmeyle beraber özellikle işgücü ve doğal çevre gibi ekonomik faktörlerin hesapsızca tahrip edilmesine yol açtı. Bu eleştiriler kurumsal sosyal sorumluluk ve sürdürülebilirlik kavramlarının ortaya çıkış noktası olmuştur. Eleştirilerin ikinci dayanağı ise, 'bırakınız yapsınlar' ilkesi gereğince devlet müdahalelerinin olmadığı ekonomik sistemin, görünmez el metaforuyla öne sürüldüğü gibi kendi kendine dengeye ulaşmak bir yana, hem ülkeler çapında hem de dünya çapında, özellikle günümüz ekonomik ortamında sıklıkla tekrar eden ekonomik krizler doğurmasıdır. 1929 yılında yaşanan Büyük Buhran bu krizlerin en ünlüsüdür. 2008 yılı küresel ekonomik krizi ise, en sonuncusudur.

Smith'in görünmez elinin umulduğu gibi ekonomik sistem içinde kaynakların en verimli şekilde kullanılmasını sağlamadığının ve piyasayı dengeye getirmediğinin anlaşılması, hükümetlerin ekonomiye müdahalesinin zorunlu bir gereklilik olduğunu ortaya çıkarmış, bunun sonucu olarak da ekonomik sistemin en önemli aktörleri olan

işletmelerin uymak zorunda olduğu yasalar ve düzenlemelerin sayısı giderek artmıştır. Küreselleşmenin etkisini giderek arttırması, teknolojide yaşanan gelişmeler ve uluslararası ticaret hacminin devasa boyutlara ulaşması, işletmeleri ulusal yasa ve düzenlemelerin yanında, çok sayıda uluslararası düzenlemeyle de karşı karşıya bırakmıştır. Artık küçük ölçekli işletmeler bile, yasalar ve düzenlemeler ağıyla örülü karmakarışık bir dünyanın içerisindedirler.

Diğer taraftan bu karmakarışık ekonomik düzen, işletmeleri risk unsurlarıyla örülü bir işletme çevresiyle yüz yüze getirmiştir. Bu ortamda işletme için gelecekte ortaya çıkabilecek problemlerin önceden saptanması ve yönetilmesi son derece önem arz etmektedir. Sayıları giderek artan ve sürekli değişen düzenlemelerin risk unsurlarını artırması, risklerin saptanması ve yönetilmesinin önemini artıran sebeplerden sadece birisidir. Küresel ekonomik sistem, özellikle büyük ölçekli işletmeleri, ülke riski gibi kontrol edilemeyen risk faktörlerinin ortasında bırakmıştır. Bu anlamda ekonomik krizler sebebiyle hassaslaşan ve giderek daha da karmaşıklaşan piyasalar, işletmeler arasında yaşanan yoğun rekabet ve sayıları giderek artan zorunlu veya gönüllü düzenlemeler; işletmeler için etkili risk yönetimi yapmayı kaçınılmaz hale getirmiştir. Bu durum risk yönetimini, sürekli değişen ekonomik konjonktürde, kesinlikle uygulanması gereken işletme standartlarından biri yapmıştır.

Devlet düzenlemelerinin olmadığı piyasaların kendiliğinden dengeye gelmediğinin artık iyice anlaşılmaya başlandığı dönemde, sanayi devrimiyle artan büyük işletme sayısı ve buna bağlı olarak artan sermaye ihtiyacı, işletme üzerindeki menfaat sahiplerinin sayısını artırmıştır. Artan sermaye ihtiyacı, işletmelerin çok sayıda ortağın bir araya gelerek kurulmasına, bunun da ötesinde bu ihtiyacın hisse senedi satarak giderilmeye başlanmasına yol açmıştır. Bu durum işletmenin sahipliğiyle yönetiminin birbirinden ayrılmasına neden olmuştur. İşletme yöneticiliği, sahipler tarafından yerine getirilmemesi gereken profesyonel bir meslek haline gelmiştir. Ancak değişen şartlar, bazı sorunları beraberinde getirmiştir. Adam Smith'in Ulusların Zenginliği kitabında ifade ettiği gibi, yöneticilerden başkalarının paralarını harcarken, kendi paralarını harcarken gösterdikleri özeni göstermeleri beklenemez (Smith, 1838, s.586). Sahiplik ve yöneticiliğin birbirinden ayrılması, sahiplerin hatta değişen şartlar sonucunda sayıları artan diğer işletme paydaşlarının, iyi işletme yönetimi için yöneticileri kontrol etmelerini ve denetlemelerini bir zorunluluk haline getirmiştir. Özellikle 2000'li yıllarda yaşanan yolsuzluklar ve

muhasebe skandalları bu durumu perçinlemiş, iyi yönetişim ve paydaşların haklarını gözeten kurumsal anlayışlar ortaya çıkmıştır.

Ekonomik sistem ve işletme dünyasında tarihsel süreçte ortaya çıkan dönüşüm, günümüzde işletmeler açısından birçok gerekliliğin ortaya çıkmasına sebep olmuştur. Daha önce de ifade ettiğimiz gibi, işletmeleri yakından etkileyen bu gereklilikler üç temel konu etrafında gelişmektedir. (1) Günümüz işletme çevresi birçok ulusal ve uluslararası düzenlemeyle örülüdür ve işletmeler bu ortamda faaliyetlerini yürütebilmek için bunlara uyum sağlamak zorundadır. Bu zorunluluk ancak iyi bir uygunluk yönetimiyle başarılabilir. (2) Küreselleşme sonrasında ekonomik sınırların ortadan kalktığı ve dünyadaki işletmelerin birbiriyle rekabet etmek zorunda kaldığı ekonomik sistem, birçok riski bünyesinde barındırmaktadır. İşletmeler ancak etkili risk yönetimiyle bu riskleri önceden saptayabilecek ve yönetebileceklerdir. (3) İşletmelerin değişen sahiplik yapısı ve buna bağlı olarak ortaya çıkan sermaye şirketleri, işletme yöneticiliğinin sahiplerin ve diğer paydaşların haklarını koruyacak şekilde geliştirilmesini zorunlu hale getirmiştir. Artık işletme yöneticileri, tüm çıkar sahiplerinin haklarını korumayı amaçlayan kurumsal yönetişimi benimsemek zorundadır.

Yukarıda bahsettiğimiz yeni ihtiyaçlara cevap verebilmek için uygunluk, risk yönetimi ve kurumsal yönetişim kavramları tarihsel süreçte birbirinden bağımsız olarak gelişme göstermiş ve işletmeler, bu kavramlara ve geliştirilen standartlara uygun olarak yönetilmeye başlamıştır. Günümüz işletme çevresinde artık bu kavramların bir arada düşünülmesi ve yönetilmesi gerekmektedir. Çünkü bu kavramlar, birbirini etkileyen sorunları ele almakta ve çözüm üretmeye çalışmaktadır. Sayıları giderek artan ve sürekli revize edilen düzenlemeler sadece uygunluk yönetimi açısından önemli değildir, aynı zamanda risk yönetimi de bu düzenlemelere bir an önce uyum gösterilmesi için çalışır ve bu düzenlemeleri bir risk faktörü olarak saptar. Benzer şekilde kurumsal yönetişim, işletmenin maruz kaldığı risklerin tespit edilip, uygun seviyede tutulması amacıyla kurumsal risk çerçevesinin geliştirilmesi gerektiğini savunur. Hem küresel hem yerel ekonomik sistemi etkileyen risk unsurları; devletlerin, düzenleyici kurumların ve işletmelerin uyum sağlanması gereken yeni düzenleme ve politikalar geliştirmesinin birincil sebebidir. İşletmelerin etkin yönetişimin bir gereği olarak risk faktörlerinin doğurduğu yeni dış düzenlemelere ve iç politikalara uyum sağlaması, ancak farklı risk türlerinin kurumsal risk yönetimi aracılığıyla kontrol altında tutulmasına ve uygunluk yönetimiyle uyumun sınırlarının açıkça belirlenmesine bağlıdır.

İşletmenin başarısını doğrudan etkileyen bu üç kavramın birlikte ele alınması fikri, Yönetişim-Risk-Uygunluk (YRU) (Governance-Risk-Compliance (GRC)) kısaltmasıyla ifade edilir. Bu kısaltma bu üç alanın birbiriyle bağlantılı olarak, bütüncül bir yaklaşımla ele alınması gerektiğini savunan bir yönetim yaklaşımını yansıtır. Son on yıllık süreçte ortaya çıkan ve giderek gelişme gösteren bu yaklaşıma; denetim-danışmanlık firmaları, akademisyenler ve teknoloji satıcıları kayıtsız kalmamıştır. Akademisyenler ve danışmanlık firmaları tarafından, YRU yaklaşımının işletmelerde daha iyi uygulanabilmesi için modeller ve çerçeveler geliştirilmiş ve teknoloji satıcıları tarafından, işletmelerin bilgi teknolojileri altyapılarının bu yaklaşıma uyum sağlaması için YRU yazılımları geliştirilmiştir.

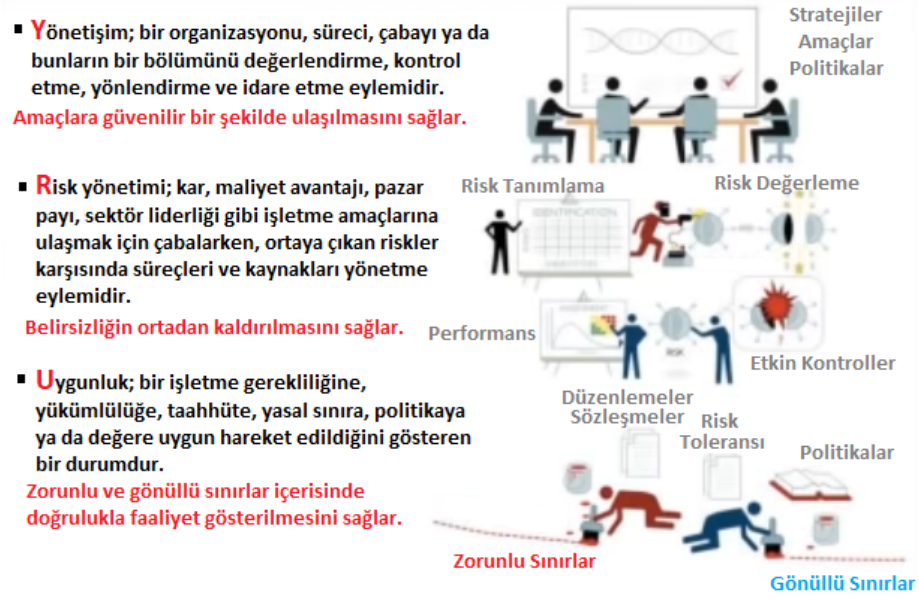
### 3.1. YRU (Yönetişim-Risk Yönetimi-Uygunluk) Kavramı

YRU kavramı ilk defa 2004 yılında küresel çapta muhasebe, denetim ve danışmanlık firması Price Waterhouse Coopers tarafından kullanılmıştır (Price Waterhouse Coopers, 2004; Wu vd., 2016, s. 2; Vicente ve Da Silva, 2011, s. 199). İlk defa kullanıldığından bu yana kavramın özellikle teknoloji satıcıları, analistler ve danışmanlar tarafından kullanımı giderek artmaktadır (Marks, 2010, s. 25). YRU kısaltması günümüzün karmaşık işletme çevresinde, organizasyonu yönlendirmekten ve yönetmekten sorumlu herkesin üzerinde düşündüğü ya da düşünmesi gereken önemli bir işletme kavramı haline gelmiştir (IIA, 2010b, s. 1).

Büyük ölçekli şirket sahtekârlıkları ve iflaslar, yakın geçmişte gerçekleşen küresel finansal krizler, çevre felaketleri, sayıları giderek artan yasal düzenlemelerin getirdiği zorunluluklar, kurumsal itibar riskinin daha etkili yönetilmesi ihtiyacı ve paydaşlar tarafından hesap verebilirliğin kapsamının genişletilmesinin talep edilmesi yönetişim, risk yönetimi ve uygunluk ile ilgili işletme sorunlarının çözümünde kapsamlı ve bütüncül bir yaklaşım olan YRU kavramının ileri sürülmesine yol açmıştır (Hardy & Leonard, 2011, s. 2).

Ayrı ayrı ele alındıklarında yönetişim, risk yönetimi ve uygunluk yeni kavramlar değildir. Şeffaflığı ve hesap verebilirliği artırmaya çalışmak, riskleri azaltmak, yasal düzenlemelere uyum sağlamak her zaman işletmelerin uğraşmak zorunda olduğu konular olmuştur ve işletme yöneticilerinin temel endişelerindendir. Fakat bu kavramlar stratejik amaçlarına ulaşmaları için işletmelere destek sağlayan bütün gereksinimlere uyum sağlamayı da kapsayacak şekilde bütüncül bir bakış açısıyla YRU olarak ele

alındıklarında, işletme faaliyetlerine daha fazla değer katma ve rekabet avantajı sağlama potansiyeline ulaşırlar. Yani aslında yeni olan, bütünleşik bir kavramlar seti olarak ortaya çıkan YRU bileşenlerinin algılanışıdır (Price Waterhouse Coopers, 2005, s. 16). YRU yaklaşımının bütünleştirdiği kavramlar Şekil 3.1'de gösterilmiştir.




**Şekil 3.1.** *YRU Yaklaşımının Bütünleştirdiği Kavramlar*

YRU kavramı tanımlayıcı ve normatif olarak iki farklı anlamda kullanılır (Hardy & Leonard, 2011, s. 3). Tanımlayıcı anlamda YRU bir sistem (OCEG, 2009, s. 2), bir yaklaşım (Marks, 2010, s. 25; Racz vd., 2010, s. 111) ve riskleri yöneterek, yasalara ve düzenlemelere uyum sağlayarak yönetişimi geliştirmek için belirlenen bir amaç (Proctor & Caldwell, 2011, s. 4) olarak görülür. Paydaşların beklentilerini karşılamak, performansı geliştirmek ve etik hareket etmeyi sağlamak gibi birçok amaca hizmet eder. Normatif anlamda ise YRU, bir YRU projesinin kapsamını belirlemek ve projeyi ele almak, bir YRU sistemini ya da bu sistemin bir yönünü kurmak ve yönetmek veya daha iyi anlamak için (Frigo & Anderson, 2009a, s. 22) işletmelere destek sağlayan bir model veya çerçeve olarak görülür (OCEG, 2009, s. 9).

Literatürde yönetişim, risk ve uygunluk (YRU) konusunda az sayıda bilimsel çalışma bulunmaktadır (Papazafeiropoulou & Spanaki, 2015, s. 1). Son yıllarda bilimsel anlamda da YRU'ya olan ilgi giderek artmaktadır. YRU konusunda ilk bilimsel tanım 2010 yılında Racz vd. tarafından yapılmıştır. Racz vd. (2010) yaptıkları çalışmada literatür incelemesi ve çevrimiçi uzman anketi aracılığıyla kapsamlı bir YRU tanımı

türetmiştir: YRU; strateji, süreçler, teknoloji ve çalışanların düzenlenmesiyle işletmenin etik olarak doğru hareket etmesini ve risk yaklaşımı, iç politikalar ve dış düzenlemeler ile uyumlu olmasını sağlayan, böylece etkinliği ve verimliliği geliştiren işletme çapında yönetişim, risk yönetimi ve uygunluğu sağlamayı amaçlayan bütünleşik, bütüncül bir yaklaşımdır.

Açık Uygunluk Etik Grubu (OCEG) YRU sözlüğündeki tanıma göre; YRU bir organizasyonun dürüstlükle hareket ederken (uygunluk) ve belirsizliği ortadan kaldırırken (risk yönetimi) amaçlarına güvenilir bir biçimde ulaşmasına olanak tanıyan (yönetişim) yeteneklerin bütünleşik olarak bir araya getirilmesidir. YRU yönetişim, güvence, performans yönetimi, risk ve uygunluğu kapsar (http://www.oceg.org/grc-glossary/).

Kurucu üyeleri arasında SAP, Price Waterhouse Coopers, Ernst&Young, Deloitte, Microsoft ve Dell gibi işletmeler bulunan kar amacı gütmeyen bir düşünce kuruluşu olan Açık Uygunluk ve Etik Grubu (OCEG) tarafından sunulan tanım nispeten kısa bir zaman periyodunda araştırmalarda ve pratikte önemli bir referans noktası haline gelmiştir (Hardy & Leonard, 2011, s. 3). Bu tanımda YRU çalışanlar, süreçler ve teknolojiden oluşan bir sistem olarak ifade edilmiştir ve işletmenin aşağıdaki faydaları kazanmasını mümkün kılar (OCEG, 2009, s. 8):

- Paydaşların beklentilerini anlar ve bunlara öncelik verir.
- Değerler ve risklerle uyumlu işletme hedeflerini belirler.
- Riski optimize ederken ve değerleri korurken işletme hedeflerine ulaşmayı sağlar.
- Yasal düzenlemelerin, etik standartların, işletmenin taraf olduğu sözleşmelerin ve işletme politikalarının dayattığı sınırları aşmadan işletmenin faaliyetini sürdürmesine destek olur.
- Bilgilendirilmesi gereken paydaşlara ilgili, güvenilir ve zamanında bilgi sunar.
- Sistemin etkinliğinin ve performansının ölçülebilmesine olanak tanır.

OCEG kaynaklarının YRU alanında kısa sürede referans haline gelmesinin belki de en önemli sebebi OCEG tarafından geliştirilen tanımın İç Denetim Enstitüsü'nün (IIA) yaptığı iç denetim tanımıyla olan benzerliğidir. IIA'nın Uluslararası İç Denetim Mesleki Uygulama Standartları iç denetimi, organizasyonun yönetişim, risk yönetimi ve iç kontrol süreçleri üzerinde güvence sağlamak olarak tanımlamıştır. Bunlar esas itibariyle iki ince farklılıkla birlikte YRU'daki aynı süreçler ve faaliyetler setidir. YRU'nun yönetişim bileşenine organizasyon tarafından yönlendirilen ve denetlenen süreçler, önlemler,

politikalar, yapı, kültür, değerler ve misyon dahilken, IIA yönetişim konusunda yönetim kurulu tarafından yürütülen faaliyetlere odaklanmıştır. Ayrıca, OCEG'e göre YRU yönetişim, risk ve uygunluğu temsil ederken; kontroller üçünün de içinde yer almaktadır. IIA ise yönetişim, risk ve kontrollere odaklanmıştır; uygunluk risk yönetiminin kapsamında risk unsurlarından birisi olarak görülür (Marks, 2010, s. 25-26).

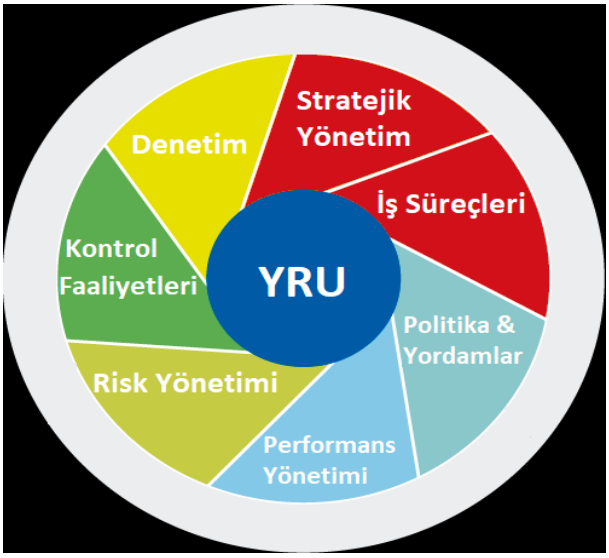
YRU yaklaşımının amacı, işletme faaliyetlerinin yürütülmesi için gerekli olan bilginin organizasyon içinde yer alan iç denetim, risk yönetimi, uygunluk gibi fonksiyonlar tarafından kullanılabilirliğini sağlarken, işletme politikalarının ve yordamların açık bir şekilde belirlenen yükümlülüklere uygun bir şekilde geliştirilmesini sağlamaktır. YRU otomatik işleyen bir risk yönetimi, iç politikalara ve dış düzenlemelere uygunluğu sağlayan ve gerektiğinde değişen koşullara adapte olan bir sistem ve organizasyon kültürüdür (Senal & Aslantaş Ateş, 2018, s. 286).

YRU işletme yönetimi ve kurumsal yönetişim yaklaşımında bir paradigma değişimini yansıtır. İşletmenin hem yasalar hem de yönetim kurulu ve üst yöneticiler tarafından belirlenen gerekliliklere uyum sağlayarak hedeflerine ulaşmasını sağlamak için kaynaklarını (insan kaynakları, teknoloji ve finansal kaynaklar) nasıl kullanabileceğine ilişkin yapısal ve felsefi bir görüş ortaya koyar. YRU yaklaşımı, işletmenin hedeflerini açıkça belirlemesini, riskleri tanımlayarak ve gerekliliklere uyum sağlayarak bu hedeflere etkili ve verimli bir şekilde ulaşmasını sağlar. Sadece uygunluğun değil, diğer YRU amaçlarının da başarılmasına hizmet eder (Mitchell, 2008, s. 70).

YRU yönetişim, risk yönetimi ve uygunluk için kullanılan bir şemsiye kavramdan daha fazlasıdır (Racz vd., 2010, s. 110). YRU kısaltması bütünleşik bir kavram olarak yönetişim, risk ve uygunluğu ifade eder ve yıllık denetimin düzenlenmesinden, iç kontrolü sürekli izleme yordamlarının kurulmasına; işletme süreçlerinde rollerin ve sorumlulukların belirlenmesinden, veri analitiği yordamlarının geliştirilmesine kadar farklı işletme faaliyetlerini kapsar (Papazafeiropoulou ve Spanaki, 2015, s. 1).

YRU süreçleri strateji geliştirme, performans yönetimi, risk yönetimi ve finansal raporlamadan iç kontrol ve bilgi teknolojisi güvenliğine kadar yönetim kurulu ve üst yönetimin sorumlu olduğu birçok faaliyeti içerir. Kısaca YRU bir denetim işinde incelenmesi gereken her şeydir. OCEG'e göre karakteristik bir YRU sisteminde bulunan fonksiyon ve süreçler şunlardır (Marks, 2010, s. 25): Yönetişim, Strateji ve İşletme Performans Yönetimi, Risk Yönetimi, Uygunluk, İç Kontrol, Kurumsal Güvenlik, Hukuk, Bilgi Teknolojisi, İşletme Etiği, Sürdürülebilirlik ve Kurumsal Sosyal

Sorumluluk, Kalite Yönetimi, Beşeri Sermaye ve Kültür, Denetim ve Güvence, Finans. YRU Yaklaşımının doğrudan ilişkili olduğu unsurlar Şekil 3.2'de gösterilmiştir.




**Şekil 3.2.** *YRU Yaklaşımının Doğrudan İlişkili Olduğu Unsurlar*

Daha önce de ifade ettiğimiz gibi, YRU üç harfli bir kısaltmadan çok daha fazlasıdır. Aslında yönetişim, risk ve uygunluktan daha fazla süreç YRU yaklaşımında önemli rol oynar. Yasal düzenlemeler ve işletme politikalarından kaynaklanan sınırları aşmadan hedeflere ulaşılması için işletmeye katkı sağlayan YRU ile ilişkili süreçler ve bu süreçlerde önemli rol oynayan çalışanlar şöyle özetlenebilir (Mitchell, 2007, s. 282-283):

1. ***Yönetişim***: Yönetişim süreçleri genellikle yönetim kurulu üyeleri, yönetim kurulu genel sekreteri ve yönetişim uzmanları tarafından yürütülür ve yönetim kurulunun yönetimi, paydaş/hissedar ilişkileri, kurumsal hedefler karşısında performansın ayarlanması ve değerlendirilmesi, stratejinin ayrıntılı şekilde incelenmesi, yönetici performanslarının değerlendirilmesi, risk gözetimi gibi konuları kapsar.
2. ***Strateji***: Strateji süreçleri genellikle genel müdür (CEO), üst düzey yöneticilerin tümü ve strateji uzmanları tarafından yürütülür ve stratejinin geliştirilmesini, dengeli kurumsal karnelerin (balanced scorecard) tasarlanmasını, kurumsal performansın yönetilmesini, birleşme ve satın alma faaliyetlerini kapsar.
3. ***Risk Yönetimi***: Risk yönetimi süreçleri genellikle riskten sorumlu yönetici (CRO) ve risk birimindeki yöneticiler tarafından yürütülür ve tüm risk türlerinin (stratejik

risk, finansal risk, operasyonel risk, uygunluk riski gibi) tanımlanmasını, değerlendirilmesini ve yönetilmesini, sigortaların satın alınmasını kapsar.

4. ***Denetim***: Denetim süreçleri genellikle iç denetim birimi yöneticisi (CAE), iç denetim birimi ve bağımsız denetçiler tarafından yürütülür ve iç denetimin yönetilmesini, bağımsız denetimin kolaylaştırılmasını, finansal raporlama yapılmasını, iç kontrollerin değerlendirilmesini (finansal raporlama üzerindeki iç kontroller ve diğer riskler üzerindeki tüm iç kontroller) ve ilgili soruşturmaları yapmayı kapsar.
5. ***Hukuk***: Hukuki süreçler genellikle hukuk müşaviri (CLO) ve hukuk birimi çalışanları tarafından yürütülür. Süreçler; hukuki stratejilerin belirlenmesini, işletmeye karşı açılan ve işletmenin açtığı davaları, işletmeye karşı yürütülen soruşturmaları, satın alma ve birleşme süreçlerinde karşıdaki şirketin finansal durumunu ve performansını ortaya çıkarmak için yapılan özen denetimini (due diligence) ve yasalara uygunluğun sağlanmasını kapsar.
6. ***Uygunluk***: Uygunluk süreçleri genellikle hukuk müşaviri, uygunluktan sorumlu yönetici (CCO), etik ve uygunluk uzmanları ile diğer hukuk çalışanları tarafından yürütülür. Süreçler; istihdam, çevre, devlet düzenlemeleri, uluslararası ticaret, hileyi önleme, yolsuzluğu önleme, bilgi gizliliği ve güvenliği, satış uygulamaları (anti-tröst sorunları), reklam ve pazarlama, ürün ve üretim kalitesi gibi konularda uygunluğu kapsar.
7. ***Bilgi Teknolojisi***: Bilgi teknolojisi süreçleri genellikle bilişimden sorumlu yönetici (CIO) ile bilgi gizliliği ve güvenliği çalışanları tarafından yürütülür ve otomatik kontrolleri, elektronik kayıtların yönetimini, iç ve dış raporlamayı kolaylaştırmayı, bilgi güvenliğini ve bilgi gizliliğinin sağlanmasını kapsar.
8. ***Etik ve Kurumsal Sosyal Sorumluluk***: Süreçler genellikle etikten sorumlu yönetici ve varsa sosyal sorumluluktan sorumlu yönetici tarafından yürütülür. Davranış kurallarının ve etik liderliğin geliştirilmesini, benimsenen ilkelerin ve değerlerin teşvik edilmesini, kamuoyuyla iletişimin ve raporlamanın geliştirilmesini, sosyo-politik ve ekonomik şartların anlaşılmasını, insan davranışlarının düzeltilmesini kapsar.
9. ***Kalite Yönetimi***: Kalite yönetimi süreçleri kalite uzmanları tarafından yürütülür ve işletmenin tamamında yalın düşüncenin geliştirilmesi, süreç geliştirme projeleri ve

sorunun kaynağını bulma analizlerinin yönetilmesi, tüm işletme süreçlerinde altı sigma ve diğer tekniklerin geliştirilmesi gibi konuları kapsar.

10. ***İnsan Sermayesi ve Kültür***: Süreçler genellikle insan kaynağı uzmanları ile örgütsel tasarım ve geliştirme uzmanları tarafından yürütülür ve işgücü yeteneklerinin geliştirilmesi, bireysel ve takım performanslarının değerlendirilmesi, doğruluk, açıklık, hesap verebilirlik ve çalışma kültürünün geliştirilmesini kapsar.

Yukarıda sıralanan alanların her biri işletmenin OCEG'in ifadesiyle ilkeli performansa ulaşmasında anahtar rol oynar. Bunların her biri, YRU amaçlarına ulaşmak için paylaşılan strateji ve teknolojiden, operasyonel yaklaşımdan ve işletme içi iletişimden faydalanır (Mitchell, 2007, s. 283).

Sonuç olarak YRU, bakış açısına bağlı olarak farklı anlamları ya da bu anlamların hepsini birden ifade edebilen kapsamlı bir kavramdır. (1) YRU işletmenin yönetişim, risk yönetimi ve uygunluk yönetimi süreçlerini bir arada düşünen ve bu şekilde hem kaynakların daha etkin kullanılmasını hem de rekabet avantajı sağlamayı öngören bir yaklaşım, yönetim disiplini, anlayış ya da felsefedir. (2) Bu yaklaşımın işletmelerde daha kolay ve anlaşılır şekilde oturtulması için kullanılan bir çerçevedir. Aynı zamanda da (3) YRU yaklaşımının işletmelere kazandırılması için gereken teknik altyapıyı sunmak için geliştirilen bir teknoloji çözümüdür. Farklı bakış açılarıyla yapılmış birçok YRU tanımının olmasının temel sebebi de budur.

### 3.2. YRU Yaklaşımının Ortaya Çıkış Nedenleri

Günümüzün işletme iklimi daha önce hiç olmadığı kadar karmaşık ve zorlayıcıdır. İşletmeler artık bugünün işletme iklimiyle de baş etmek zorundalar. Devlet kurumları, kar amacı gütmeyen kuruluşlar, hatta küçük işletmeler bile geçmişte yalnızca çok büyük uluslararası işletmeleri etkileyen sorunlarla karşılaşmaktalar. İşletmelerin uğraşmak zorunda olduğu değişimin ortaya çıkmasına sebep olan faktörlerden bazıları şunlardır (OCEG, 2015a, s. 1):

- Paydaşlar sadece yüksek performansı değil, işletme faaliyetlerinde şeffaflığı da talep etmekteler.
- Yasal düzenlemeler ve zorunluluklar sürekli değişmektedir ve bu değişim tahmin edilemez bir hal almıştır.

- Katlanarak artan risklerin ve hem işletme içinde hem de talep zincirinin bir parçası olarak işletme dışında giderek artan üçüncü taraf ilişkilerinin yönetilmesi güçleşmiştir.
- Tehditlerin ve fırsatların etkisini tahmin etmek zorlaşmıştır.
- Riskler, yasalar ve işletme politikalarından kaynaklanan gereklilikleri gidermenin maliyeti kontrolden çıkmıştır.
- Bir organizasyonun hem içindeki hem dışındaki değişimin hızı ve büyüklüğü karşı konulamaz hale gelmiştir.

İşletmeleri YRU yaklaşımını uygulamaya güdüleyen güçler şöyle sıralanmıştır (Broady & Roland, 2008, s. 14-20):

***Finansal Düzenlemelere Uygunluk***: Birçok ülkede yeni yasal düzenlemelere göre finansal raporlarda ciddi hataların bulunması, sorumluların cezai kovuşturmayla karşı karşıya kalmasına neden olmaktadır. Gelişmiş ülkelerin birçoğu, finansal raporlama ve kontroller hakkında detaylı inceleme gerektiren yasal mevzuatlara sahiptirler. Örneğin, Sarbanes-Oxley iç kontrol konusunda birçok düzenleme getirmiştir. Bu düzenlemelerin arkasındaki yönlendirici güç, kusurlu finansal raporlamanın finansal sisteme zarar vereceği endişesidir. Finansal raporlamayı ve yönetişimi geliştirmeyi hedefleyen yasal düzenlemelere uyum sağlama çabaları, işletmeleri açıkça YRU'ya yönlendirmektedir.

***Denetim Başarısızlıkları***: Yaşadığı denetim başarısızlıkları, işletmeleri YRU süreçlerini geliştirme yönünde teşvik etmektedir. Kamuya açıklanan finansal tablolar hakkında olumsuz görüş bildirilen bir denetim sonrasında, yatırımcılar işletmeye olan güvenlerini kaybederler ve hisselerini satmak isterler. Günümüzde, denetimler eskiden olduğundan daha fazla nedenle başarısızlıkla sonuçlanmaktadır. Bir hilenin ya da başka bir kötü niyetli davranışın ortaya çıkarılması kesinlikle en olumsuz nedendir. Denetim problemleri; yeterli kontrollerin eksikliği, görevlerin uygun şekilde ayrılmaması, finansal raporlar hazırlanırken yetersiz gözetim ve diğer birçok neden yüzünden ortaya çıkabilir. Başarısız bir denetim sonrasında, raporlama gereklilikleri artar. Normalde yıllık yapılan kontroller çeyrek yılda bir ya da ayda bir yapılabilir. Genellikle yeni kontroller geliştirilir. Bu yeni faaliyetlere ilişkin işlerin tamamı şirket çalışanları tarafından veya bir denetim veya danışmanlık firması aracılığıyla yapılır. Öyle ya da böyle maliyetler artar. Başarısız bir denetim sonrasında artan maliyetler işletmenin kontrolleri ve testleri daha kolay ve ucuza yapabilmek amacıyla YRU süreçlerini otomatikleştirmesi için güçlü bir güdüleyicidir.

***YRU İhtiyacının Farkına Varmak***: İşletmeleri YRU performanslarını geliştirmeye iten başka bir güdüleyici de, bazen bir dış inceleme aracılığıyla ortaya çıkabilir. Bağımsız denetçilerin denetim sürecinde yaptıkları sorgulamalar, işletmelerin YRU ile ilgili konularda sistemlerinin zayıflıklarını keşfetmelerine olanak verir. Genellikle bu zayıflıklar, çalışanların yasa ve düzenlemelerin taleplerini anlamamalarından ya da bu talepleri karşılamak için kullanılan mevcut sistemin karmaşıklığından kaynaklanabilir. Ayrıca YRU ile ilgili ihtiyacın ortaya çıkmasına olanak veren inceleme, bazen de üst yönetim, yönetim kurulu, yeni çalışanlar, iç denetçiler ve diğer şirket çalışanları tarafından da yapılabilir.

***Ortaklık Yapısındaki Değişimden Kaynaklanan Yeni İhtiyaçlar***: İşletmeler ortaklık yapılarını değiştirerek ilk defa halka açılacakları zaman bir takım raporlama ve yönetişim gerekliliklerıyle karşılaşırlar. İşletmelerin hisselerini satabilmek ve ortaklık yapıları gereği uymak zorunda oldukları yeni yasal düzenlemelere uyum sağlayabilmek amacıyla yönetişim ve raporlama seviyelerini yükseltmeleri gerekir. Ortaya çıkan yeni işletme ihtiyaçları YRU süreçlerinin geliştirilmesini gerektirir.

***Büyümeyi Yönetmek***: Etkileyici bir büyüme eğrisine sahip küçük işletmeler, yeni çalışanları işe alırken işletmenin finansal durumuna zarar verilmediğinden emin olmak için genellikle YRU'dan yararlanırlar. Yönetim, uygun kontroller ve testler geliştirerek, yeni çalışanlar anahtar görevler üstlendiğinde, işletmenin risk altında olmadığından emin olabilir.

***Güvence Sağlamak***: Yeni sahipleri bir işletmeyi devraldığında, YRU uygulamak her faaliyetin düzgünce yürütüldüğünden ve hileli bir şeylerin gerçekleşmediğinden emin olmanın en kesin yöntemlerinden birisidir. YRU yeni sahiplere güvence sağlar. Eksiksiz YRU uygulamanın bir parçası olarak geliştirilen kontroller ve testler, işletmenin finansal açıdan doğru yönetildiğini ve muhasebe raporlarının işletmeye doğru olarak iletildiğini garanti eder.

***Riskleri Yönetmek***: Sık sık kötü sürprizlerle karşılaşan işletmeler, potansiyel operasyonel riskleri tanımak ve yönetmek için bir erken uyarı sistemi geliştirme yolu olarak YRU süreçlerini ve otomasyonlarını geliştirirler. YRU'yu sadece bir finansal kavram olarak düşünmek büyük bir hatadır. Korkunç finansal sonuçlara neden olabilen riskler, asla bilançoda gözükmeyen birçok operasyonel faktör sebebiyle de ortaya çıkabilir. Örneğin, YRU'nun risk yönetim süreçleri, bir üretim tesisinin yedek parça

deposunda önemli bir parçanın kritik seviyeye düşmesi gibi finansal olmayan bir soruna da çözüm sağlar.

***Maliyetleri Azaltmak***: Yönetişim, risk yönetimi ve uygunluk ile ilgili maliyetleri azaltma arzusu işletmeleri YRU'ya yönlendiren başka bir önemli güdüleyicidir. YRU konusunda eğitimli çalışan azlığı ile kontroller ve testlere ilişkin analizler ve raporlama yapmak amacıyla hizmet alınan şirket dışından danışmanlara ve denetçilere yapılan harcamaları göz önüne alarak, birçok işletme bir maliyet azaltma yöntemi olarak YRU uygulamaya çalışmaktadır. Bazı işletmeler bu şekilde maliyetlerini yüzde 20'den fazla azalttıklarını açıklamışlardır.

***Artan Uygunluk İhtiyaçları***: Risk sadece finansal konularla ilgili bir kavram olarak kalmadığı gibi, uygunluk da sadece finansal düzenlemelere uyum sağlamak ile ilgili değildir. Giderek hızlanan küreselleşmenin bir sonucu olarak, örneğin herhangi bir yerde üretilen mallar başka bir yere gönderilebilir ve uygunluk gereklilikleri bu malların taşınmasını sağlamak için çok önemlidir. Her bir sınır ötesi yer değişimi, izinin sürülmesi ve kaydedilmesi gereken çok sayıda belgenin düzenlenmesini ve çok fazla farklı tarafla ilgilenilmesini gerektirebilir. Ayrıca güvenlik sorunları da işin başka bir boyutudur. Mallar gönderilmeden önce, hükümetin kendisine mal göndermeyi yasakladığı kişiler ve işletmeler listesi kontrol edilmelidir. Çevresel düzenlemeler de giderek artan bir biçimde uygunluğun odak noktası haline gelmektedir. İşletmelerin uyum sağlamak zorunda olduğu, hem ulusal hem de uluslararası düzeyde özellikle tehlikeli maddeler ile ilgili çevresel düzenlemelerin sayısı sürekli artmaktadır. Sayıları giderek artan ulusal ve uluslararası düzenlemeler ve uyum sağlama zorlukları, işletmeleri YRU'ya yönlendiren bir başka önemli sebeptir.

### 3.3. İlkeli Performans

Açık Uygunluk ve Etik Grubu'nun (OCEG) ifadesiyle YRU, 'ilkeli performansa' ulaşılmasını sağlayan bir yetenektir. İşletmelerin en geniş kapsamlı amacı ilkeli performansa ulaşmaktır. İlkeli performans, belirsizliği ortadan kaldırarak ve dürüstlükle hareket ederek, işletmenin güvenilir bir şekilde amaçlarına ulaşmasını sağlayabilmek, olarak tanımlanmıştır (Switzer vd., 2013, s. 3). İlkeli performansa bir işletmenin hem finansal hem de finansal olmayan hedeflerini ve bu hedeflere ulaşırken işletmenin aşmaması gereken sınırları açısından belirsizliklerin giderilmesi, bu hedefler doğrultusunda ve sınırlar içinde kalmasını sağlayan yöntemlerin, net olarak ifade

edilmesiyle ulaşılır. İlkeli performans; etik performans, ekonomik performans ve kurumsal sosyal sorumluluğun daha da ötesine geçer. Bir işletme için doğru olanın yanında, doğru olan eylemleri yapmak için doğru yöntemlerin de tanımlanmasıyla İlkeli Performansa ulaşılabilir. Geleneksel bakış açısının tersine, işletmenin amaçlarına ulaşması için değerleri oluşturmanın yanında, onları korumak için belirlenen sınırları aşmadan nasıl hareket etmesi gerektiği konusundaki belirsizliğin de ortadan kaldırılması gerekir (Mitchell, 2008, s. 69-70).

İlkeli performans, bir OCEG markasıdır ve jenerik bir ifadedir. Kavramdaki performans sözcüğü işletmenin ekonomik ve ekonomik olmayan amaçları doğrultusunda yürüttüğü faaliyetlerini belirtir. İlkeli sözcüğüyse söz konusu faaliyetlerin işletme içerisinde geliştirilen politika, yordam ve etik kodlara ya da işletme dışından dayatılan yasal düzenlemelere veya günümüz karmaşık işletme çevresinde sürekli olarak değişim gösteren tehdit ve fırsatları dikkate almak amacıyla bir zorunluluk haline gelen risk yönetimi gerekliliklerine bağlı kalınarak yürütülmesini ifade eder. Kısaca faaliyetlerin belirlenen ilkelere bağlı kalınarak yürütülmesidir.

İşletme içinde başarıyı mümkün kılan sağlam ve enerjik duruma ulaşılmasını ifade eden ilkeli performansa ancak ortak amaçlar düzenlenerek, işletme içinde arzulanan kültür geliştirilerek, bilgi ve çekirdek fonksiyonlar bütünleştirilerek ve bunlar güçlü bir iletişim ve etkili teknolojiyle desteklenerek ulaşılabilir. Geliştirilen amaçlar doğrultusunda güçlü bir şekilde çaba göstermek yeterli değildir. Başarı için potansiyel riskler ve fırsatlardan kaynaklanan belirsizlikler, toplumsal adetler ve yasal sınırlar dikkate alınmalıdır. Performans yönetimi; risk, uygunluk ve etik amaçları belirleme faaliyetinden ayrı düşünülmemelidir (OCEG, 2015a, s. 3).

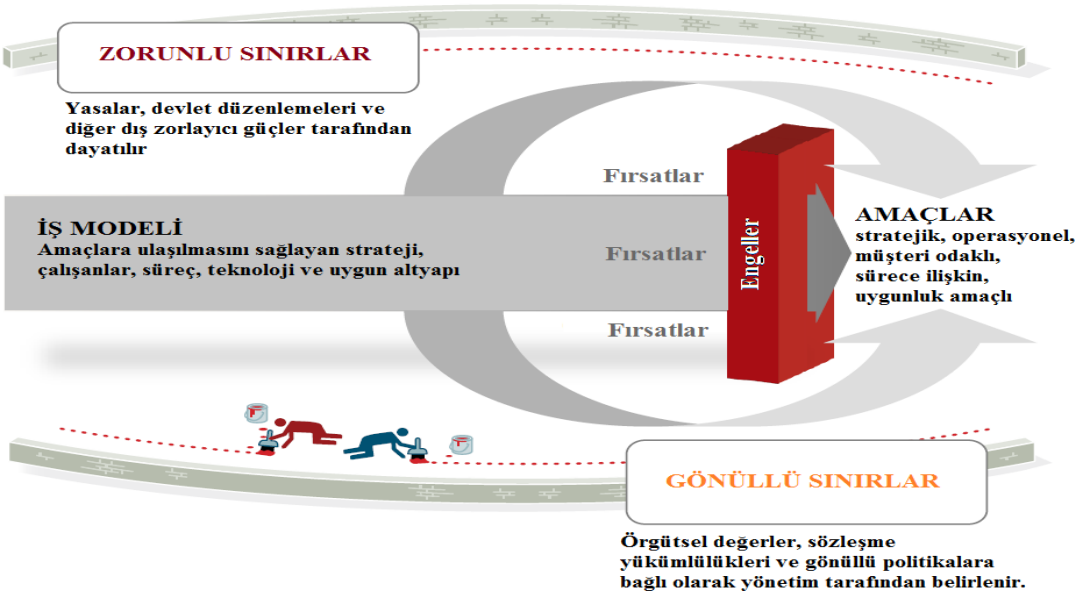
İlkeli performans, performans yönetimiyle ilişkilidir. Risk yönetimi, uygunluk ve etik amaçları performans yönetimiyle ilişkilendirir. Bir işletme belirli ölçütler altında ekonomik veya ekonomik olmayan amaçlarına ulaştığını sanabilir. Ancak belirlenen ölçütler risk yönetimi, uygunluk ve etik göz ardı edilerek düzenlenmişse optimal performansa ulaşıldığı söylenemez. Yani performans yönetimi süreci risk yönetimi, uygunluk ve etikten bağımsız olarak değerlendirilemez. Söz konusu faktörlerin öne sürdüğü sınırlar (ilkeler) dikkate alınmak zorundadır. Ayrıca performans yönetimi sürecinden elde edilen sonuçlara bağlı olarak işletme, risk yönetimi ve iç kontrol faaliyetlerini yönlendirmelidir. Saptanan bir başarısızlık veya performans düşüklüğü bir

risk faktörü olarak ele alınmalı ve olumsuz sonuçları engellemek amacıyla eylemler ve kontroller geliştirilmelidir.

İşletmenin faaliyetlerine rehberlik eden sınırlar zorunlu (işletme dışından dayatılan yasalar, düzenlemeler ve diğer gereklilikler) veya gönüllü (işletmenin değerleri ve politikaları) olabilir. Bu sınırları çabucak anlayabilmek, işletme için çok önemlidir. İşletmeler her zaman bunların içerisinde faaliyet gösterirler. Bu sınırlarda meydana gelen değişiklikler ilkeli performansa ulaşan bir işletme tarafından açık biçimde takip edilir. En nihai YRU amacı olan ilkeli performans, işletmenin hangi amaçların peşinden koşması gerektiği ve bu amaçları nasıl takip edeceği konusunda daha fazla esneklik sağlayan bir yönetim disiplinidir. Bir işletmede ilkeli performansa erişmek aşağıdaki faaliyetleri yerine getirdiği için önemlidir (Mitchell, 2007, s. 280-281):

- İşletmenin ilkeleri açıkça tanımlanır.
- İşletmenin ulaşması gereken amaçlar belirlenir.
- Amaçlara nasıl ulaşılacağı tespit edilir.
- Risklerin ve belirsizliklerin nasıl ortadan kaldırılacağı, değerlerin nasıl korunacağı ve faaliyetler süresince, belirlenen davranış sınırları içerisinde nasıl kalınacağı ortaya konur.
- İç ve dış paydaşlar için istenen seviyede şeffaflık sağlanır.
- En yüksek düzeyde performansa ulaşılması için, yukarıdaki faaliyetlerin hepsi sürekli olarak geliştirilmeye çalışılır.

Şekil 3.3, ilkeli performansa ulaşan işletmelerin iş modellerini zorunlu ve gönüllü sınırlarla çevrelenen işletme çevresinde fırsatlara ve engellere karşılık verebilmek amacıyla düzenleyebileceklerini göstermektedir.




**Şekil 3.3.** *İlkeli Performans (Mitchell, 2010, s. 26)*

İlkeli performansa ulaşmak için, organizasyonlar amaçlarına ulaşmalarını destekleyen davranış ve olayları proaktif bir şekilde teşvik etmeli ve bu amaçlara ulaşmanın önündeki her türlü tehdidi engellemelidir. Ayrıca, hedeflere doğru devam eden süreçler tespit edilmeli ve ortaya çıkan ya da ortaya çıkma ihtimali beliren istenmeyen davranışlar, koşullar ve olaylar belirlenmelidir. Nihayetinde, organizasyon istenen ve istenmeyen davranışlar, koşullar ve olaylara uygun şekilde karşılık vermelidir (Mitchell ve Switzer, 2016, s. 11). Bu amaçla işletme içinde ortaya çıkan veya ortaya çıkma ihtimali olan davranış, koşul ve olayları tespit eden ve bunlara gerektiği gibi tepki veren uygun kontroller geliştirilmelidir.

İlkeli performans her işletmenin ulaşmak için çaba göstermesi gereken bir YRU yeteneğidir. Bu yeteneğe ulaşarak YRU yaklaşımından elde edilen fayda en uygun seviyeye çıkarılabilir. Bir işletmenin en geniş kapsamlı YRU amacı olan ilkeli performansa ulaşarak elde edeceği on temel fayda aşağıda sıralanmıştır (OCEG, 2015a, s. 11):

1. İşletme amaçlarına ulaşılması: İşletmenin amaçlarına ulaşılması için işletmenin bütün parçalarının birlikte çaba göstermesini sağlar.
2. Amaçların ve stratejik planlamanın risk bilinciyle düzenlenmesinin sağlanması: Bütün seviyelerde yürütmeden sorumlu işletme yöneticilerine, stratejik planlamacılara ve yönetim otoritelerine riskler, fırsatlar ve sorumluluklar hakkında zamanında, güvenilir ve kullanışlı bilgi sağlar.

3. Örgütsel kültürün yaygınlaştırılması: Performans, hesap verebilirlik, dürüstlük, güven ve iletişim kültürünü geliştirir ve destekler.
4. Paydaşların güveninin artırılması: Paydaşların işletmeye olan güvenini geliştirir.
5. İşletmeyi koruma: Olumsuzluklara ve sürprizlere karşı işletmeyi korurken ve fırsatların değerlendirebilmesini sağlarken, işletmeyi risklere ve gerekliliklere cevap verebilmesi için hazırlar.
6. Zayıflıkları ve güçlükleri önleme, bulma ve azaltma: Potansiyel problemleri tespit etmek ve etkilerini azaltmak, olumsuz çıktıları önlemek ve ortaya çıkan sorunları gidermek için eylemler ve iç kontroller geliştirir.
7. Yapılması istenen davranışları motive etme ve destekleme: Özellikle zorlayıcı şartlarla karşılaşıldığında yapılması istenen davranışların teşvik edilmesini ve yapılması halinde ödüllendirilmesini sağlar.
8. Rakiplerinden daha avantajlı konumda olma: Engeller ve tuzakların üstesinden gelmek amacıyla yapılan stratejik ve taktik yönlendirmelerdeki hızlı değişimleri desteklemek için gereken bilgi düzeyine ulaşılmasını sağlar.
9. Duyarlılık ve verimliliği geliştirme: Rekabet avantajı elde etmek için işletmenin tümüyle daha duyarlı ve verimli olmasını sağlayan yetenekleri geliştirir.
10. Ekonomik getiri ve değerleri optimize etme: Yatırımlar ve faaliyetlerde insan kaynaklarını ve finansal kaynakları işletmenin ekonomik getiri ve değerini maksimize edecek şekilde düzenler.

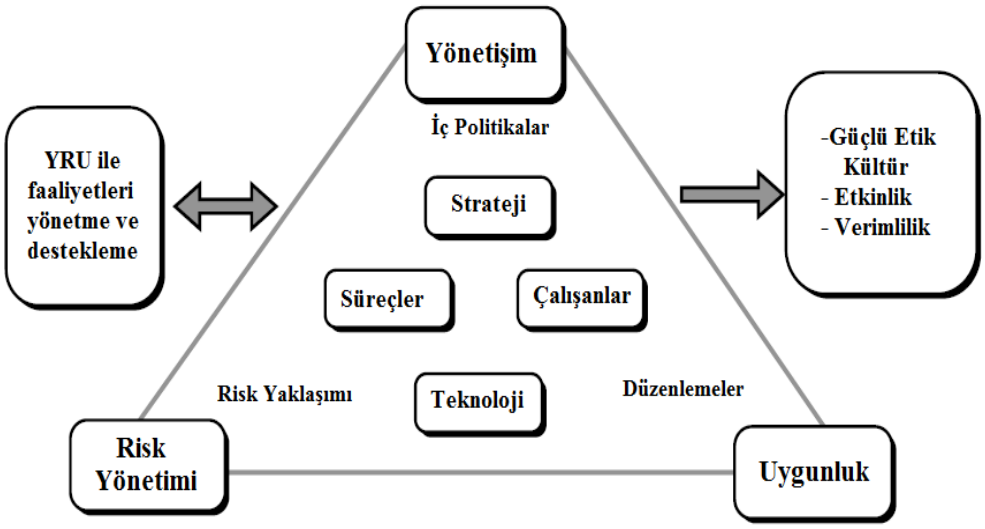
### 3.4. YRU Bileşenleri

Kurumsal risk yönetiminin etkin bir şekilde uygulanmasını sağlamak amacıyla, dünyadaki birçok ülkede risk yönetimi, yönetişim kodlarının önemli bir parçası haline gelmiştir. Birçok ülke kendi yönetişim kodlarını, standartlarını ve risk yönetimi çerçevelerini hazırlamaktadır. Bu kod ve çerçeveler; dolandırıcılık, müşteri hizmetleri, paydaşların gereksinimleri ve şirket performansı ile ilgili davranış standartlarını düzenler ve işletmelere rehberlik sağlar. Risk yönetimi, açık bir şekilde yönetişim standartlarıyla bağlantılıdır ve yönetim kurulunun kilit bir sorumluluğu olarak gösterilmiştir. Bu düzenlemeler halka açık şirketlere uygulanmaktadır ve bazı gereklilikler yasallaştırılmışken, bazıları sadece önerilmektedir. Zorunlu veya gönüllü olarak uygulanması amaçlanan kodlara, çerçevelere ve standartlara uyum için etkin bir uygunluk yönetimi gereklidir.

Yönetişim ve risk yönetimi birbiriyle ilişkili ve birbirlerine bağlıdır. İşletme performansının istikrarı ve iyileştirilmesi, her iki bileşenin etkili rolü üzerine büyük oranda bağımlıdır. Kontrol bileşeni yönetişimin sorumluluklarından birisidir ve sağlam kontrol ortamı risk yönetimi süreciyle geliştirilebilir. Bu bağlamda yönetişim, amaçlarını gerçekleştirme doğrultusunda faaliyet gösterirken organizasyonu bir arada tutan bir yapışkan olarak görülebilir. Risk yönetimi ise bu sürece esneklik sağlar. Aslında, kurumsal risk yönetimi kavramı ve pratikleri, yönetişimi güçlendirmek için kullanılan hayati bir araçtır (Knight, 2006, s. 11).

Yönetişim, etkin risk yönetimi için hayati önem taşımaktadır ve uygunluk yönetimi olmadan tüm risk yönetimi bileşenleri eksik kalır. Yönetişim; pay sahipleri, yönetim kurulu, üst yönetim ve paydaşlar arasındaki ilişkileri normalleştirir. İşletme amaçlarına ulaşmak ve hissedar değerini en üst düzeye çıkarmak için yönetişim, risk yönetimi ve uygunluk arasındaki bütünleşmeye ihtiyaç duymaktadır. İşletmeler, yönetişim ve risk yönetimi ile ilgili kural, düzenleme, politika ve standartlara uymak zorundadırlar. Uygunluk, kurumsal risk yönetiminin önemli bir tamamlayıcı unsurudur ve katma değere dayalı etkin bir kurumsal dönüşümün uygunluğu desteklemesi gerekir. Uygunluk ilgili tüm kanunlara, düzenlemelere ve işletme politikalarına uyum gösterilip gösterilmediğini denetlerken; yönetişim, işletmenin maruz kaldığı riskleri yönetmek için doğru işletme altyapısını geliştirir (Manab vd., 2010, s. 242).

Daha önce de vurguladığımız gibi, şemsiye bir kavram olan YRU, bir işletmenin yönetişim, risk yönetimi ve uygunluk faaliyetlerini kapsar ve bu faaliyetlerin bütüncül bir bakış açısıyla ele alınması gerektiğini savunur. Ancak bu faaliyetlerin her biri günümüz işletme dünyasının hem değişimine yön vermiş, hem de değişen ihtiyaçları karşısında çözüm olarak ayrı ayrı öne sürülmüştür. Bu bileşenleri bütünleştiren YRU yapısı, Şekil 3.4'te gösterilmiştir.




**Şekil 3.4.** *YRU Temel Bileşenler (Moeller, 2011, s. 23)*

Bu bileşenler farklı konulara odaklanmış ve her biri işletme içinde dağınık faaliyetlere sahip olsalar da, bunlar arasında bağlantılar vardır. Örneğin, birçok işletme, yasal düzenlemelerin işletmelere dayattığı örgütsel rehberler tarafından da istendiği şekilde, etik ve kültür kavramlarına uygunluk programları içinde yer vermelerine karşın, yönetişim de bir özellik olarak kültürün korunmasını açıklar ve işletme içinde etik davranışların geliştirilmesi gerektiğini savunur (OCEG, 2009, s. 9).

YRU Kavramı; yönetişim, risk yönetimi ve uygunluk bileşenlerini sıkıca birbirine bağlar. Şekil 3.4'te görüldüğü gibi, uygunluk bileşeni yasal düzenlemeleri yönlendirir, risk yönetimi işletmenin risk yaklaşımının anahtar bileşenidir ve iç politikalar yönetişimin desteklenmesinde esas faktördür. Bu üçgenin içinde, stratejiler, etkili süreçler, bilgi teknolojilerini de kapsayacak biçimde teknolojiler ve hepsinden önemlisi çalışanlar yer alır. Şeklin sağ tarafı, bir işletmede yönetimin işletmenin yordam ve politikalarına uyulmasında rol oynayan kurum kültürünü kapsayacak şekilde doğru etik davranışa, örgütsel etkinlik ve verimliliğe dikkat etmesini ve bunları desteklemesi gerektiğini gösterir (Moeller, 2011, s. 23).

Bir işletmenin yönetişim, risk yönetimi ve uygunluk yönetimi faaliyetlerine bütüncül bir bakış açısı getiren YRU yaklaşımı, farklı konulara odaklanmış ve her biri işletme içinde dağınık faaliyetlere sahip olan YRU bileşenlerinin arasındaki örtüşmeleri ve bağlantıları ortaya çıkarır. Bu yaklaşım, işletmelerin söz konusu süreçlerde daha etkin

ve verimli olmasını ve işletme amaçlarına ulaşılmasında birbirinden bağımsız hareket eden süreçleri bütünleştirerek rekabet avantajı ve maliyet etkinliği elde etmesini destekler.

### 3.4.1. Yönetişim / Kurumsal Yönetim

Yönetişim halka açık ya da halka açık olmayan, kamu ya da özel bir organizasyonun süreçler, sistemler ve kontrollerini geliştirir. Latince kökenli bir kelime olan 'Yönetişim' (Governance), idare etmek anlamına gelir ve tipik olarak, yasalara ve düzenlemelere uyulmasını ve organizasyonu yönetmek için kurumsal kaynakların kullanılmasını kapsar. Sahipliğin ve kontrolün birbirinden ayrılmasını savunan bir çalışma alanıdır. Yönetişim; yönetim kurulları, işletme ortakları, yöneticiler, çalışanlar, müşteriler ve düzenleyici kurumlar arasındaki ilişkileri düzenler (Tarantino, 2008, s. 2).

Yönetim kurulu ve üst yönetime; muhasebe ve finansal raporlama sisteminin etkin işlediği ve güvenilir çıktılar ürettiği, işletme için gerekli iç kontrolün oluşturulduğu ve faaliyetlerinin verimliliği hakkında bekledikleri güvenceyi sağlayabilecek en etkili araçlardan biri iç denetim işlevidir. İşletmelerde şirket yönetim kurulunun pay ve menfaat sahiplerine karsı sorumluluklarını etkin bir biçimde yerine getirebilmesi için, iç denetim faaliyeti olmazsa olmazdır (Uzun, 2011, s. 28). İç denetim pay ve menfaat sahiplerinin işletme faaliyetleri hakkında yeterli, doğru ve zamanında bilgi almalarını sağlamak amacıyla üst yönetime tavsiyeler getirebilir.

#### *3.4.1.1. Yönetişimin / Kurumsal yönetimin ortaya çıkışı*

Sanayi Devrimiyle başlayan makineleşme ve bunun sonucunda daha büyük üretim tesislerinin ortaya çıkmaya başlaması işletmelerin sermaye ihtiyacını artırmıştır. İlerleyen dönemde işletmelerin sermaye ihtiyacı az sayıda ortağın gideremeyeceği seviyelere yükselmiştir. Bu durum işletmelerin paylarının finansal piyasalar aracılığıyla yatırımcılara sunulmasına yol açmış ve işletme sahipliğinin az sayıda kişi tarafından elde tutulmasının önüne geçmiştir. Kaldı ki işletme payları karlı görülmesi nispetinde bireysel yatırımcıların yanında kurumsal yatırımcılar tarafından da satın alınmaya başlamıştır. Böylece işletmelerin ortaklık yapıları eskiye nazaran çok sayıda yatırımcı tarafından oluşmaya başlamıştır. Ayrıca küreselleşmenin bir sonucu olarak fon hareketlerinin dünya genelinde dolaşım gücüne kavuşması, işletme paylarının dünyanın her yerinden bireysel ve kurumsal yatırımcılar tarafından elde tutulabilmesinin önünü açmıştır.

Ortaya çıkan yeni ekonomik dünya düzeni, ortak olmanın ve ortaklıktan ayrılmanın eskiye nazaran çok daha kolay olduğu, alacaklılarına karşı sınırlı sorumlu sermaye şirketlerini ortaya çıkarmıştır. Sermaye şirketlerinin dünyanın her yerinden çok sayıda ortağa sahip olmaları neticesinde ortaya çıkan problemler, daha profesyonel bir yönetime ihtiyaç duyulmasına yol açmış ve bunun doğal bir sonucu olarak sahiplik ve yöneticilik birbirinden ayrılmıştır.

Dünya genelini etkileyen Enron, Tyco, Worldcom, Parmalat gibi yolsuzluk skandalları, gelişen bu ekonomik düzene olan güvenin sorgulanmasına yol açmıştır. Küçük pay sahiplerinin çıkarlarının büyük hissedarlara ve yöneticilere karşı korumasız oluşu, bu yolsuzlukların yaşanmasına ve sisteme olan güvensizliğin vahim boyutlara ulaşmasına sebep olmuştur. Güven ortamının tekrar tesis edilmesi ve ekonomik sistemin eskisi gibi işlemesi için yönetişim / kurumsal yönetim kavramı ortaya atılmıştır. Bu kavram işletmelerin hem tüm menfaat sahiplerinin haklarını korumasını garanti eder hem de işletmenin daha profesyonel olarak etkin ve verimli çalışabilmesini sağlayan bir sistem geliştirmesinin yolunu açar.

Küreselleşen dünyada uluslararası sermaye hareketlerinin ve ekonomik ilişkilerin gelişmesi, işletmelerin artan sermaye ihtiyaçlarını giderek daha fazla oranda küçük hissedarlar ve kurumsal yatırımcılar aracılığıyla karşılamaya başlaması, işletmelere yatırım yapan hissedarların işletme yönetimine etkin olarak katılamaması ve dolayısıyla da çıkarlarını ana sermayedar ve yöneticilere karşı koruyamamaları sorunu, yönetim kurullarının, CEO'ların ve genel müdürlerin kararlarının giderek daha fazla önem kazanması gibi sebepler kavramın ortaya çıkışında etkili olmuştur.

Günümüz dünyasının değişen ekonomik düzeninde sayıları giderek artan özellikle büyük ölçekli ve çok ortaklı işletmelerde sistemin doğal bir sonucu olarak sahiplik ve yönetim fonksiyonlarının kaçınılmaz olarak birbirinden ayrılması ve gelişen işletme çevresinde işletme kurucularının ve ana sermayedarlarının diğer pay sahiplerinin temel mülkiyet haklarını göz ardı ederek sahiplik ve denetim fonksiyonlarını kendi çıkarlarına hizmet edecek şekilde kullanmaları kavramın bilimsel anlamda doğuşuna ortam ve meşruiyet kazandırmıştır (Aktan, 2006, s.7). Nitekim dünyayı sarsan yolsuzluk skandallarında ortaya çıktığı gibi söz konusu hakların kurucular, ana sermayedarlar ve yöneticiler tarafından suiistimal edildiğinin ortaya çıkması, yönetişimi dünya çapında çok fazla tartışılan bir konu haline getirmiştir.

Yönetişim işletme faaliyetlerinde kar sağlamak ve pay sahiplerine kazanılan karı dağıtmak olan geleneksel yaklaşımın esas amacıyla birlikte, hissedar ve yöneticileri de kapsayacak şekilde tüm çıkar sahiplerinin haklarının savunulması ve bu çerçevede söz konusu çıkar grupları arasındaki ilişkilerin düzenlenmesini amaçlayan bir kavramdır (Şehirli, 1999, s.8). Yönetişimi ortaya çıkaran işletmelerin ortaklık yapılarını değiştiren şartlar, geleneksel yönetimin yetersizliklerini ortaya çıkarmış ve bunun yerine yönetişimin gerekliliğini göstermiştir.

Yönetişimin esas amacı, yöneticilerin bütün işletme paydaşlarının özellikle de mevcut ve potansiyel yatırımcıların menfaatlerini koruyacak tarzda çalışmasını ve işletmenin finansal durumuna ilişkin doğru ve eksiksiz açıklamaların zamanında yapılmasını sağlamaktır. Ancak bu şekilde tüm yatırımcılar için güven ortamı tesis edilir, şeffaf ve doğru açıklamalar ile sermaye maliyeti düşürülür ve bireysel veya kurumsal yatırımcılar işletme için istikrarlı bir finans kaynağı haline getirilebilir (Koçel, 2003, s.466).

İşletmelerin finansal durumunun şeffaf bir şekilde yatırımcılara raporlanmasında, faydalı finansal bilginin niteliksel özellikleri olan gerçeğe ve ihtiyaca uygun biçimde karşılaştırılabilirlik, doğrulanabilirlik, anlaşılabilirlik ve zamanında sunum bilginin kalitesini artıracaktır. Etkin bir yönetişimin / kurumsal yönetimin tesis edilmesi, ancak yüksek seviyede finansal bilginin paydaşlara iletilmesiyle sağlanabilir.

#### *3.4.1.2. Yönetişim / Kurumsal yönetim kavramı*

Kavram yönetişim, kurumsal yönetim, kurumsal yönetişim, iyi yönetim veya iyi yönetişim olarak da ifade edilmektedir. Bu terimler İngilizce 'corporate governance' kavramının dilimize çevrilmesi sonucu ortaya çıkmıştır. Bunlardan hangisi kullanılırsa kullanılsın ifade edilmek istenen hep aynı yönetim ve yaklaşım biçimidir (Aysan, 2007, s.20). Ancak kavramın kökenindeki yönetim kavramı resmi otorite tarafından desteklenen faaliyetlere vurgu yaparken, yönetişim ortak paylaşılan amaçlarla beslenen uygulamalara işaret eder.[5] Ayrıca yönetim, hükmetme güç ve yetisine sahip birimleri tanımlarken, yönetişim bunun dışındaki resmi olmayan örgütlenmeleri de içinde barındırır. Yönetimle

[5] Yönetişim, yönetim kavramını tanımlamakla birlikte demokratiklik, açıklık, hesap verme, çoğulculuk ve kararların en yakın örgütsel seviyede verilmesine de işaret eder (Leftwich, 1993, s.605). Yönetişim, yönetime katılım fonksiyonu kazandırmıştır.

karşılaştırıldığında yönetişimin kapsamı daha geniş bir çerçeveye oturur (Rosenau, 1992, s.3-6).[6]

Dünya Bankası'nın tanımına göre yönetişim, bir işletmenin finansal ve beşeri sermayeyi kendisine çekerek ve faaliyetlerini etkin şekilde yürüterek, hem ait olduğu toplumun değerlerine saygı gösterip hem de uzun vadede işletme ortaklarına ekonomik değer yaratmasına imkân sağlayan her türlü kanun, yönetmelik, kod ve uygulamalardır (IFC, 1999, s.11).

OECD'ye göre yönetişim, ekonomik verimlilik ve büyümeyi artırmanın ve aynı zamanda yatırımcı güveninin kazanılmasının anahtarıdır. Bir işletmenin yönetim kurulu, pay sahipleri ve diğer tüm menfaat sahipleri arasındaki ilişkileri düzenler. Yönetişim aynı zamanda işletmenin amaçlarının belirlendiği, bu amaçlara nasıl ulaşılacağının ve performansın nasıl denetleneceğinin belirlendiği bir yapıyı ortaya koyar. İyi yönetişim, yönetim kurulları ve üst yönetim için işletmenin ve hissedarlarının menfaatleri doğrultusunda amaçlara yönelme açısından uygun teşvikleri sağlamalı ve etkin denetimi kolaylaştırmalıdır (OECD, 2005, s. 9).

OCEG'in yaptığı tanıma göre yönetişim, işletme tarafından yönlendirilen ve kontrol edilen kültür, değerler, misyon, yapı, politikalar ve tedbirlerdir. Bu bağlamda, yönetişim, yönetim kurulunun tüm faaliyetlerini kapsar. Ayrıca işletmenin çeşitli seviyelerinde bulunan yönetişim organları da önemli rol oynar. Bir yönetişim tarzının düzenlenmesi, uygulanması ve üst yönetimle iletişimi sağlaması önemli bir başarı faktörüdür (OCEG, 2009, s. 9).

Yönetişim, işletmenin doğru yönde idare edilmesi ve politikalar, yordamlar ve süreçlerin ihtiyaç duyulan biçimde geliştirilmesiyle ilgilidir. İşletmenin ihtiyaç duyduğu stratejinin ne olduğu ve nasıl geliştirileceğiyle ilgilenir. Yönetişim bir şirketin yürüttüğü tüm faaliyetlerin yanı sıra uygunluk ve risk yönetimi faaliyetlerini de organize eder. Ayrıca, YRU süreçlerinde analiz edilen ve işletmeyi geliştirmek için kullanılan verinin nasıl elde edileceğiyle de ilgilenir. Üst yönetim seviyesinde yönetişim, doğru ürünlerin doğru pazarlarda satılması gibi daha genel konularda işletmenin idare edilmesiyle ilgilenir. Yönetişim, yönetim kurulu ve üst yönetim tarafından geliştirilen stratejinin

[6] Kavram yazında daha fazla çalışmada kurumsal yönetim olarak kullanılsa da, geleneksel yönetim yaklaşımının aksine, yönetim uygulamalarının sorumluluklarını sadece yönetime yüklememesi yani yönetilenlerinde yönetime katıldığı bir yönetim tarzını savunması ve yönetişim kavramının daha geniş bir çerçeveyi ifade etmesi nedeniyle yönetişim olarak kullanılması gerektiğini savunuyoruz. Çalışmamızda da kavram bu tespitten sonra böyle kullanılmıştır.

tercüme edilmesi (alt kademeye işleriyle bağlantılı olarak anlayacakları biçimde iletilmesi) için vardır (Broady & Roland, 2008, s. 31).

Yönetişim bir işletmenin yönetim kurulu, yöneticileri, çalışanları, hissedarları, tedarikçileri, bağlı olduğu ticaret toplulukları ve devlet kurumlarının dâhil olduğu tüm paydaşlarıyla ilişkilerini koruyan ve düzenleyen bir süreçtir. Yöneten ile yönetilen arasındaki ilişkileri ifade eder. Ayrıca bu sürece, kimin yöneteceği, kimin yönetileceği ve hangi kaynakların kullanılacağına ilişkin üç temel karar verme konusu da dâhildir (Tarantino, 2008, s. 3).

Yönetişim ilk defa adının geçtiği resmi belge olan Cadbury Raporunda "işletmeleri idare ve kontrol eden bir sistem" olarak tanımlanmıştır. Bu tanımda işletmeleri idare ve kontrol etme olarak ifade edilen işletme yönetiminden en üst seviyedeki organ olan yönetim kurulları sorumludur. Yönetim kurullarının görevi stratejik amaçları belirleyerek ve uygulanmasını sağlayarak işletme yönetimine liderlik etmek, denetlemek ve bunu pay sahiplerine raporlamaktır. Pay sahiplerinin yönetimdeki sorumluluğu ise, yönetici ve denetçileri görevlendirmektir. Yönetim kurullarının görevleri genel kurulda pay sahiplerinin alacağı kararlarla beraber kanunlara ve düzenlemelere bağlıdır (Cadbury Report, 1992, s.14).

İşletme Sektörü Danışma Grubu başkanı M. Ira Millstein'in geliştirdiği yaygın kabul gören tanıma göre; *"yönetişim bir işletmenin hak sahipleri ve toplum çıkarlarına zarar vermeyecek şekilde, mali kaynakları ve insan kaynaklarını işletmeye çekmesini, verimli çalışmasını ve bu sayede de hissedarları için uzun dönemde ekonomik kazanç yaratarak istikrar sağlamasını mümkün kılan kanun, yönetmelik ve ilgili gönüllü özel sektör uygulamalarının bileşimidir. "*

Bu bağlamda yönetişim, işletmelerin sermayeyi ve insan kaynaklarını çekmesine, etkin performans göstermesine, amaçlarına ulaşmasına, hukuki zorunlulukları ve kamuoyu beklentilerini yerine getirmesine yönelik yasa, düzenleme ve gönüllü özel sektör uygulamalarından oluşur (Deloitte, 2006, s.4).

Dar anlamda yönetişim; hissedarların ve kreditörler, tüketiciler, çalışanlar, sendikalar, tedarikçiler ve devlet organları gibi diğer tüm paydaşların haklarının işletme tarafından korunması ve bu hakların sahipleri tarafından etkin kullanılmasını sağlayan sistemlerin kurularak işletmenin yönetilmesidir (Güçlü, 2010, s.1).

Yönetişim en geniş anlamda iyi şirket yönetimi için gereken formel ve informel kurallar bütünü olarak tanımlanabilir. Kısa ve öz bir ifadeyle iyi işletme yönetimidir. İyi

işletme yönetimi için yönetimin görev ve sorumluluklarının belirlenerek tüm paydaşların haklarının azami seviyede korunmasını da sağlayan yasal yaptırımlara bağlanması gerekli olmakla beraber yeterli değildir. İyi yönetişim için bunların da ötesinde değişim yönetimi, stratejik yönetim, sinerjik yönetim, toplam kalite yönetimi, insan kaynakları yönetimi gibi yönetim ilkelerinin ve yönetim tekniklerinin uygulanması gerekmektedir (Aktan, 2006, s.5).

#### *3.4.1.3. Yönetişimin kapsamı*

İşletmenin içindeki yönetişim süreçleri kurumsal ilkeleri, anahtar politikaları, risk yaklaşımını tanımlar ve birbirleri arasındaki bağlantıyı kurar, işletmenin uyguladığı çerçevelerin izlenmesini sağlar ve tanımlanan rehberler ve ilkeler kapsamında işletmenin performansını değerlendirir. Risk felsefesi ve yaklaşımı, iş etiğine uygunluk, kurumsal politikalara uygunluk, işletme performansının raporlanması ve kurumsal sosyal sorumluluk bir yönetişim programında bulunması gereken anahtar bileşenlerdir (Switzer vd., 2013, s. 11).

Yönetişim sadece üst yönetim ve yönetim kurulu üyelerinin tüm paydaşlar için kurallar geliştirmesinden çok daha fazlasıdır ve paydaşların bu kurallara da uymasının sağlanmasını kapsar. İşletmenin ihtiyacı olan doğruluk, güven, dürüstlük, açıklık, sorumluluk ve hesap verebilirliği, karşılıklı saygı ve işletmeye bağlılığı geliştirir. Yönetişimin kapsadığı konular şunlardır (Moeller, 2011, s. 115):

***Dürüstlük ve Etik Davranış***: Etik ve sorumlu karar alma sadece halkla ilişkiler için değil, risk yönetimi ve uygunluk faaliyetleri için de gereklidir. Bir işletme; üst yöneticileri, birim yöneticileri ve diğer paydaşları arasında etik ve sorumlu karar almayı teşvik etmek amacıyla davranış kuralları geliştirmelidir. İşletme bu pratikleri desteklemek ve yönetişimi geliştirmek için, etik ve yasal sınırlar dışında adımlar atılabilecek alanlarda riskleri minimuma indirecek uygunluk ve etik programları uygulamalıdır.

***Kamuyu Aydınlatma ve Şeffaflık***: İşletmeler hissedarlar ve diğer paydaşlar seviyesinde hesap verebilirliği sağlamak için üst yönetimin ve yönetim kurulunun rol ve sorumluluklarını açık bir şekilde belirlemeli ve kamuoyuyla paylaşmalıdır. Ayrıca kurumsal finansal raporlamanın doğruluğunu bağımsız biçimde onaylayan ve koruyan yordamları uygulamalıdır. Finansal ve diğer önemli konularda kamuyu aydınlatma, tüm yatırımcıların ve ilgili paydaşların doğru ve tam bilgiye erişebilmelerini sağlamak amacıyla zamanında ve eksiksiz sunulmalıdır.

***Hissedarların Hakları ve Eşit Muamele***: Bir işletme hissedarlarının ve diğer paydaşlarının haklarına saygı duymalıdır ve bu hakların korunmasını desteklemelidir. Etkili bilgi iletişimi için anlaşılabilirliği ve erişilebilirliği sağlayarak ve açık iletişimi teşvik ederek, bu hakların gerektiğinde kullanılmasına yardımcı olmalıdır. Ayrıca bir işletme tüm hukuki paydaşlarına karşı yasaların ve diğer yükümlülüklerinin farkında olmalıdır.

***Yönetim Kurulunun Rol ve Sorumlulukları***: Yönetim kurulu çeşitli işletme sorunlarıyla uğraşabilecek anlayışa ve yeteneklere ihtiyaç duyar ve yönetimin performansını inceleyebilme yeterliliğine sahip olmadır. Yönetim kurulu görev ve sorumluluklarını yerine getirebilecek düzeyde bilgi birikimine sahip çalışanlara ihtiyaç duyar.

#### *3.4.1.4. Yönetişimin faydaları*

Yönetişimin hem işletmelere hem de işletmeyle ilgili bütün taraflara önemli faydaları vardır. Konuya işletme açısından bakıldığında yönetişim kalitesinin yüksek olması finansal imkânların ve likiditenin artması, düşük sermaye maliyeti ve krizlerin daha kolay üstesinden gelinmesi anlamına gelir. Öte yandan, güçlü bir yönetişimin yatırımcılar açısından da faydaları vardır. Örneğin şeffaflık, yatırımcıların yatırım yapmayı planladıkları işletmeye ilişkin nitelikli, güvenilir ve anlaşılır verilere zamanında ulaşmasının önünü açar (Tüm, 2013, s. 98).

Güçlü yönetişim sermaye piyasalarının derinleşmesine de katkı sağlar. Özellikle küçük ve orta ölçekli işletmelerin kaynaklara erişimini kolaylaştırmakta ve örgütsel yapıyı değiştirerek verimliliği artırmaktadır. Ayrıca işletmede belirsizliğin azaltılmasına katkı sağlayarak, risk primini düşürmekte ve böylece kaynak sağlamayı kolaylaştırmaktadır. Düşük maliyetle kaynak bulan işletmeler daha kolay büyümekte ve paydaşlarının çıkarlarını maksimum seviyeye çıkarabilmektedir (Erdönmez, 2003, s. 43). Yönetişimin işletmelere sağlayacağı yararları şu şekilde özetleyebiliriz (Aktan, 2006, s. 14: Karakaya ve Akbulut, 2010, s. 22):

- Şirketin finans piyasalarından daha kolay kaynak elde etmesini sağlar.
- Sermaye maliyetini azaltır.
- Yerli ve yabancı yatırımcıların güvenini artırır ve böylece uzun vadeli sermaye girişi hızlanır.
- Finansal krizlerin daha kolay atlatılmasını sağlar.

- İşletme varlıklarının değeri yükselir.
- İyi yönetimle varlıkların getirisi yükselir ve işletmenin değeri artar.
- Yönetimde şeffaflık ve hesap verme sorumluluğu yolsuzlukları azaltır.
- Şirkette güç ve yetki istismarını engeller ve keyfi yönetimi ortadan kaldırır.
- Tüm paydaşların çıkarlarına hizmet edeceği için işletme ile paydaşlar arasındaki ilişkilerin ve diyalogun artmasına katkı sağlar.
- İşletme faaliyetlerinde uzun dönemli istikrar sağlar.

#### *3.4.1.5. Yönetişimin ilkeleri*

Yönetişim mikro bakış açısıyla işletme içindeki tüm tarafların haklarını korumaya odaklanır. İşletmenin en yüksek performansa ulaşmasını ve sürdürülebilir başarıyı yakalamasını amaçlar. İşletmede iyi bir yönetişim, temel ilkeleri olan eşitlik, şeffaflık, sorumluluk ve hesap verebilirliği sağlamaya yönelik bir çatı olarak düşünülebilir. Bu ilkeler ışığında yönetişim, işletmenin en yüksek performansla çalışarak, en yüksek kar ve başarıya ulaşmasında yol gösterir (TÜSİAD, 2002, s.8).

##### *3.4.1.5.1. Şeffaflık ilkesi*

Yönetişimde şeffaflık ilkesi, ticari sır niteliği taşıyan ve henüz kamuoyuyla paylaşılmamış bilgiler haricinde kalan işletmeyle ilgili tüm finansal ve finansal olmayan bilgilerin, zamanında, doğru, anlaşılabilir, yorumlanabilir, eksiksiz ve düşük bir maliyetle elde edilebilir şekilde kamuoyuna duyurulmasıdır (SPK, 2005, s.3).

Şeffaflığın yeterli düzeyde olmamasının yaşanan finansal krizlerin ortaya çıkmasının başta gelen nedenlerinden biri olduğu anlaşılmıştır. Finansal bilgilerdeki eksiklik, uyarı sistemlerinin harekete geçmesini engellemiş ve gerekli önlemlerin alınmamasına neden olmuştur. Bu yargı şeffaflık ile iyi yönetim ve ekonomik istikrar arasında güçlü ilişkiler olduğunu gösterir. Özellikle gelişmiş birçok ülkede hem finansal hem de yönetsel şeffaflığı artırmaya yönelik düzenlemeler benimsenmiştir. Çünkü kötü yönetimin yarattığı olumsuz etkiler irdelendiğinde, şeffaflığın artırılmasının hem piyasaların etkin olarak işlemesi hem de iyi yönetim anlayışının yerleştirilmesi yoluyla toplumun yararına olacağı düşünülmektedir (Tuzcu, 2004, s.18).

Etkin bir yönetişim anlayışı ve güçlü sermaye piyasalarının oluşturulması için gerekli olan temel unsur şeffaflıktır. Yatırımcılar düzenli, güvenilir, karşılaştırılabilir ve

anlaşılabilir bilgiye erişmeden kurumsal manzarayı ve işletme performansını değerlendiremezler ve çeşitli yatırım kararları arasında sağlıklı tercih yapmaları olanaksızdır (Eroğlu, 2003, s.6).

Şeffaflık hem yönetsel hem de finansal anlamda saydamlığı gerektirir. Yönetsel saydamlık her şeyden evvel yönetim kurulunun ve işletmenin örgütsel yapısındaki tüm yöneticilerin yetki dağılımının açıkça belirlenmesini ve paylaşılmasını gerektirir. Finansal saydamlık ise, işletmenin finansal yapısının ve alacağı kararların denetime elverişli ve izlenebilir olmasını gerekli kılar (Deloitte, 2008, s. 14). Yönetim kurulu işletmenin iç kontrol yapısını finansal yapının denetlenmesine elverişli bir şekilde kurmaktan sorumludur. Bu süreçte en mutlak yardımcısı iç denetimdir. Etkin bir iç kontrol yapısının oluşturulması bağımsız denetimin yürütülmesinin önünü açacak ve finansal saydamlığı sağlayacaktır. Şeffaflık ilkesinin yerine getirilmesi bağımsız denetimin etkinliğine bağlıdır. Çünkü ancak denetim sürecinin sonuçları genel kurulun bilgisine sunulduğunda pay sahiplerinin işletmenin finansal durumu hakkında doğru bilgiye ulaşması sağlanmış olacaktır.

OECD Yönetişim İlkelerine göre, yönetişim çerçevesi işletmenin mali durumu, performansı, mülkiyeti ve idaresi hakkında işletmeyle ilgili bütün maddi konularda doğru ve zamanında açıklama yapmasını sağlamalıdır (OECD, 2005, s.18). Bunu sağlamak için, finansal tabloların işletmenin ekonomik durumunu ve performansını her açıdan doğru olarak yansıttığı güvencesinin yönetim kuruluna ve hissedarlara objektif olarak verilebilmesi amacıyla yürütülen denetim faaliyetinin bağımsız, yetkin ve uzman denetçiler tarafından yürütülmesi gerektiğine işaret etmektedir (OECD, 2005, s.41).

#### *3.4.1.5.2. Hesap verebilirlik ilkesi*

Yönetişimin temel ilkelerinden bir diğeri de hesap verebilirliktir. Şeffaflık ve hesap verebilirlik bankacılık, denetim, muhasebe standartları, ulusal mali uygulamalar, uyuşturucu trafiğinin kontrolü, terörün finansmanı, çevre kirliliği, yozlaşma karşıtı çabalar, silahsızlanma girişimleri ve politika gibi çok geniş bir yelpazede tartışılmaktadır. Farklı konulardaki bu tartışmaların ortak bir amaca odaklandığı görülmektedir. Bu ortak amaç yönetimde etkinliğin artırılması yoluyla daha iyi işleyen ulusal ve uluslararası bir sistemin geliştirilmesidir (Tuzcu, 2004, s.24).

Hesap verebilirlik ilkesi işletme içinde alınan kararların doğruluğunu kanıtlama ve sorumluluğunu üstlenme gerekliliğine işaret eder. Bu ilke, yönetim işlevinin ve

sorumluklarının açıklanmasını, hissedar ve yöneticilerin taleplerinin sıraya konulmasını ve nesnel kararlar alınıp alınmadığının yönetim kurulları, üst yönetim ve diğer yöneticiler tarafından izlenmesini öngörür (Dinç ve Abdioğlu, 2009, s.160).

Hesap verme sorumluluğu iki taraf arasında güç ilişkisini belirler. Taraflardan birisi diğerine güç aktarırken, bu güce sahip olma ve kullanım hakkı karşılığında birtakım taahhütler bekler. Yetki devri sonucunda işletme birimlerinde toplanan gücün ve gücü özgürce kullanabilme fırsatının, hesap verme sorumluluğu çerçevesinde işletme faaliyetlerinde verim ve etkinlik taahhüdü ve uygun raporlama süreciyle dengeli olarak yürütülmesi zorunludur (Aydemir, 2005, s.30).

OECD Yönetişim İlkelerine göre; yönetişim çerçevesi, işletmenin stratejik rehberliğini, yönetim kurulu tarafından yönetimin etkin denetimini ve yönetim kurulunun işletmeye ve hissedarlarına karşı hesap verme yükümlülüğü taşımasını sağlamalıdır (OECD, 2005, s.19).

Hesap verebilirlik ve şeffaflık ilkeleri karşılıklı etkileşim içindedirler. Yönetimde şeffaflığın sağlanabilmesi için etkili ve iyi işleyen hesap verebilirlik süreçlerine ihtiyaç duyulur. Hesap verme süreçlerinin iyi işlemesi için de açık ve şeffaf politikalar gereklidir. Bu nedenle her iki ilke diğeri için vazgeçilmez bir araç ve önkoşuldur (Arın, Kesmez ve Gören, 2000, s.122).

Yönetişim anlayışının işletme içinde geliştirilmesi için işletmenin iyi işleyen yönetsel ve muhasebe kontrollerine ihtiyacı vardır. Etkili yönetişim için iyi işleyen bir hesap verebilirlik mekanizması şarttır. Hesap verebilirliği sağlayan temel araçlar şöyle tanımlanmıştır (Acar, 2008, s.81):

- İyi işleyen iç kontrol sisteminin oluşturulması ve düzenli olarak gözden geçirilmesi.
- İç denetim yoluyla sürekli izleme.
- Belirli aralıklarla düzenli olarak yapılan şeffaf finansal raporlama ve gözden geçirme.
- Bağımsız bir denetim komitesi tarafından denetimlerin yürütülmesi.

#### *3.4.1.5.3. Sorumluluk ilkesi*

Sorumluluk ilkesi işletme yönetiminin işletme adına yürüttüğü tüm faaliyetlerinin mevzuata, işletmenin esas sözleşmesine ve işletme içi düzenlemelere uygunluğunu ve bunların denetimini ifade eder. Bu ilke gereğince işletme içinde yetki sahibi bütün kişiler

ve organlar yürüttükleri faaliyetlerden ve aldığı kararların sonuçlarından sorumlu tutulurlar (SPK, 2005, s.3).

Sorumluluk işletmenin tüzel kişiliğinin, yönetim kurulunun ve yöneticilerinin karar ve eylemlerinin ilgili yasal mevzuata, toplumsal ve etik değerlere uygunluğunun sağlanması anlamına gelir. İyi bir işletme yönetimi için, işletme faaliyetlerinden, karar ve tercihlerinden birinci derece sorumlu olan yönetim kurulunun görev ve sorumluluklarının doğru şekilde tanımlanmış olması büyük önem taşır (Aktan, 2006, s.12).

İşletmenin sadece kanun ve düzenlemelere uyum göstererek faaliyetlerini yürütmesiyle sorumluluk ilkesine tam olarak uyulduğu söylenemez. Yönetişim kanunların sorumluluk açısından asgari standartları oluşturduğunu, gerçek anlamda sorumlu işletme davranışının yasal zorunlulukların da ötesine geçilerek yerine getirilebileceğini vurgular (TKYD, 2011, s.16). Bu bağlamda işletme içinde yetki sahibi olan kişi veya kurullar yasal düzenlemelerin ötesinde toplumsal ve etik değerlere saygı göstermeli, işletmenin başarıyla faaliyetlerini yürütmesi için gereken her türlü çabayı eylemleri ve kararlarında hem kendileri göstermeli hem de performansından sorumlu tutuldukları kişileri bu yönde teşvik etmelidirler.

Şeffaf bir yönetişim anlayışının işletme içinde hâkim olması, sorumluluk ilkesinin geliştirilmesi için büyük önem taşır. İşletme faaliyetlerinin ve işletme ile ilgili alınan kararların şeffaflık ilkesi gereği tüm paydaşlarla ve çıkar gruplarıyla paylaşılıyor olması, söz konusu faaliyetler ve kararlardan sorumlu kişiler ve kurulların sorumlulukları ölçüsünde daha dikkatli davranmalarına ve şeffaflık ilkesinin getirdiği açıklıkla sorumluluklarından kaçamamalarına sebep olacaktır.

Hesap verebilirlik ve sorumluluk ilkeleri birbirini tamamlayan etkileşim içinde bulunan ilkelerdir. Söz konusu ilkeler aynı konuya farklı pencerelerden bakarlar. Hesap verebilirlik yetkiye sahip olanlara yaptığı eylemlerin gerekçelerini açıklayabilme olanağı sunar; sorumluluk ilkesi ise yetki devredenlerin bakış açısı ile verilen görevlerin gerektiği gibi yerine getirilip getirilmediğini yani sorumlulukların uygun biçimde üstlenilip üstlenilmediğinin sorgulanmasına imkân tanır (Doğan, 2007, s.54).

#### *3.4.1.5.4. Eşitlik (Adillik) ilkesi*

İşletmenin hissedarlarının ve diğer menfaat sahiplerinin amaçları farklıdır ve aralarında çıkar çatışmalarının ortaya çıkması kaçınılmazdır. Eşitlik ilkesi işletme yönetimi tarafından birbirinden farklı çıkarlara sahip tüm taraflar arasında dengenin

sağlanmasını ifade eder (Doğan, 2007, s.51). Bu ilke sadece ana sermayedarların değil işletmeyle ilişkili bütün kesimlerin menfaatlerinin gözetilmesini gerekli kılar. İşletme yönetiminin karar alma süreçlerinde tüm tarafları dikkate alması ve bu kararlardan doğrudan veya dolaylı olarak etkilenebilecek olan bütün kesimlere eşit mesafede duracak bir tavır takınmasını gerektirir (Menteş, 2009, s.52).

İşletme yöneticileri faaliyetleri yürütürken aldıkları kararlardan etkilenen tüm taraflara karşı eşit mesafede olmalıdır. Bu adil bir yönetim anlayışının gereğidir. Yönetimin yapmış olduğu eylemlerle ilgili olarak, konuyla ilişkili açıklanabilecek nitelikteki bilginin eşanlı ve eşit bir biçimde tüm taraflar ile paylaşılması gerekir. İhtiyaç duyulan bilginin bu bilgiyi kullanacak olan işletme içinden ve dışından gruplara farklılık yaratmayacak ve hiçbirine öncelik tanımayacak şekilde aktarılması eşitlikçi yönetim göstermenin şartıdır. Ayrıca kamuoyunun kullanımına sunulan bilginin makul ölçüler dâhilinde herkes tarafından anlaşılır nitelikte olması gerekir. Aksi takdirde bilginin değerlendirilmesi konusunda eşitsizlik yaratılmış olacaktır (Tuzcu, 2004, s.25).

OECD Yönetişim İlkelerine göre yönetişim çerçevesi, azınlık ve yabancı hissedarlar da dâhil, bütün pay sahiplerine eşit muamele yapılmasını güvence altına almalıdır. Bütün hissedarlar haklarının ihlal edilmesi halinde, yeterli bir telafi ya da tazminat elde etme olanağına sahip olmalıdır. OECD'nin hissedarların adil muamele görmesi başlığı altında sıraladığı ilkeler kısaca şöyle özetlenebilir (OECD, 2005, s.16):

- Her şeyden önce tüm hissedarlara eşit muamele yapılmaya çalışılmalıdır.
- Oy haklarındaki her türlü değişiklik, bu değişiklikten olumsuz etkilen tüm hissedarların onayına sunulmalıdır.
- Azınlık hissedarların hakları korunmalı, haklarının kötüye kullanılması halinde mağduriyetlerini giderecek etkin mekanizmalar geliştirilmelidir.
- Uzaktan yapılan oylama önündeki engeller ortadan kaldırılmalıdır.
- Genel kurul toplantılarının işlem ve usulleri hissedarların eşit muamele görmesine olanak tanımalıdır.
- İçerden öğrenenlerin ticareti (insider trading) ve kötüye kullanılan çıkar amaçlı muameleler yasaklanmalıdır.
- Yöneticilerin işletmeyi etkileyen işlem ve konularla ilgili doğrudan, dolaylı ve üçüncü taraflar adına maddi çıkar konusu olabilecek her türlü ilişkilerini açıklamaları gerekmektedir.

### *3.4.1.6. Yönetişimin gelişiminde önemli rol oynayan düzenlemeler*

Bu başlıkta yönetişim kavramının ortaya çıkmasında ve gelişiminde önemli etkiye sahip düzenleme, ilke ve yasalar hakkında kronolojik sıraya uygun olarak kısaca bilgi sunulmuştur.

#### *3.4.1.6.1. Cadbury raporu*

Cadbury Komitesi 1991 yılı Mayıs ayında Finansal Raporlama Konseyi (Financial Reporting Council (FRC)) ve Londra Borsası (London Stock Exchange (LSE)) tarafından İngiltere'de kurulmuştur. Komitenin temel amacı yönetişim standartlarını geliştirmek, finansal raporlamaya ve denetime olan güven seviyesini artırmaktır. Komite Mayıs 1992'de ilk taslak raporunu kamuoyunun görüşüne sunmuştur. Komite Aralık 1992'de kamuoyunun görüşlerini de dikkate alarak raporun son halini 'Kurumsal Yönetişimin Finansal Yönleri' adıyla yayımlamıştır. Kurumsal yönetişim ifadesi ilk defa resmi olarak Cadbury Raporunda geçmektedir. Raporda genel olarak yönetişim ilkelerinin çerçevesi belirlenmiştir. Raporun geliştirdiği öneriler dünya çapında kabul edilen bir model haline gelmiştir (Şen, 2013, s.58).

Cadbury Raporunun getirdiği düzenlemelerin uygulanması yönünde bir zorunluluk yoktur. Ancak Londra Borsasına kayıtlı işletmeler, raporda yer alan direktifleri uygulayıp uygulamadıklarını, uygulamadılarsa gerekçelerini kamuya açıklamak zorundadır. Raporda yönetim kurulunun yönetici olan ve olmayan üyeleri ile raporlama ve denetime ilişkin 19 adet öneri bulunmaktadır. Raporda yönetim kurulu üyelerinin hissedarlara ve topluma olan sorumlulukları belirlenmiş, yönetişimi iyileştirmeyi ve finansal raporlama ile denetime olan güveni artırmaya yönelik öneriler geliştirilmiştir (Atamer, 2006, s.13).

#### *3.4.1.6.2. Greenbury raporu*

İngiltere'de Cadbury Komitesinin raporundan sonra 1995 yılında Sir Richard Greenbury başkanlığında Yöneticilere Yapılan Ödemeler Çalışma Grubu (The Study Group on Director's Remuneration) adıyla toplanan komite yeni bir en iyi uygulama kodu olarak gösterilen raporu yayımlamıştır. Rapor çalışma grubu başkanının adına atfen Greenbury Raporu olarak anılmaktadır ve hesap verebilirlik, sorumluluk, kamuyu aydınlatma, işletme performansı, yöneticilerin maaşları ve sağlanan diğer menfaatleri anahtar konular olarak inceler. Greenbury Raporu yöneticilere sağlanan menfaatlere

ilişkin bilgilerin işletmeler tarafından kamuya ve paydaşlara açıklanması gerekliliğini vurgular (Maassen, 2002, s.129).

#### *3.4.1.6.3. Hampel raporu*

İngiltere'de daha önce Cadbury ve Greenbury raporlarında kendisine yer bulan direktifleri incelemek ve gerekli görülürse yenilemek amacıyla 1998 yılında Sir Ronald Hampel başkanlığında, başkanının adıyla anılan bir rapor yayımlanmıştır. Hampel Raporu kendisinden önceki iki raporu ve İngiltere'deki yönetişim sistemini inceleyerek yeni bir en iyi uygulama kodu geliştirmeyi amaçlamıştır. Hampel Raporu kendinden önce yayımlanmış olan Cadbury Raporunu yenilemeye ve Greenbury Raporunda uzlaşılamamış konulara çözüm üretmeye odaklanmıştır. Sir Ronald Hampel'e göre Cadbury Raporu işletmelerin iflası, yozlaşma ve hile, Greenbury Raporu işletmelerden yöneticilere aktarılan aşırı ücret ve menfaatler gibi belirli endişeleri gidermek için geliştirilmişken, Hampel Raporu genel olarak yönetişimin geliştirilmesi için hazırlanmıştır (Maassen, 2002, s.130).

Cadbury, Grennbury ve Hampel raporları birleştirilerek Birleşik Kod hazırlanmıştır. Birleşik Kod yönetişim en iyi uygulama kodları ve bu kodların işletmeler ile diğer paydaşlara faydalarından oluşur.

#### *3.4.1.6.4. Millstein raporu*

OECD bünyesinde kurulan İşletmecilik Sektörü Yönetişim Danışma Grubu tarafından hazırlanan grubun başkanı Ira Millstein'in adıyla da anılan 'Kurumsal Yönetişim: Küresel Piyasalarda Rekabetin ve Sermaye Erişiminin Geliştirilmesi' (Corporate Governance, Improving Competitiveness and Access to Capital in Global Markets) isimli rapor 1998 yılında yayımlanmıştır. Rapor 1996 yılından beri çalışmalar yürüten danışma grubunun iki yıllık çalışmaları sonucunda hazırlanmıştır. Rapor 1999 yılında yayımlanan OECD Yönetişim İlkelerinin temelini oluşturmuştur.

#### *3.4.1.6.5. OECD Yönetişim ilkeleri*

OECD Yönetişim İlkeleri, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Konseyi tarafından ulusal hükümetler, ilgili uluslararası kuruluşlar ve özel sektör ile birlikte hazırlanmış ve 1999 yılında yayımlanmıştır. Bir dizi standart ve yol gösterici ilkeleri kapsamaktadır. İlkeler bağlayıcı olmamakla beraber hükümet ve işletmelerin kendi yönetim anlayışlarını gözden geçirmeleri ve belirlenen standartları uygulamaları açısından önemli bir rehberdir. Yönetişim kavramındaki sürekli gelişmeler ve değişen koşullar neticesinde yönetişim ilkelerinin yenilenmesi ihtiyacı ortaya çıkmış ve OECD ilkeleri 2004 yılında güncellenmiş ve yeniden yayımlanmıştır (OECD, 2005, s.3).

OECD İlkeleri, dünya genelindeki karar alıcılar, yatırımcılar, işletmeler ve diğer paydaşlar açısından uluslararası bir referans kaynağı haline gelmiştir. Onaylandığı tarihten bu yana yönetişim olgusunu gündemde tutmuş ve hem OECD üye ülkelerindeki hem de OECD üyesi olmayan ülkelerdeki yasama ve düzenleme inisiyatifleri için bir yol gösterici kılavuz olmuştur. Mali İstikrar Forumu bu ilkeleri sağlıklı mali sisteme yönelik 12 önemli standarttan biri olarak kabul etmiştir. İlkeler aynı zamanda OECD üyesi olan ve olmayan ülkeler arasındaki kapsamlı işbirliği programı için bir temel teşkil etmektedir (OECD, 2005, s.4).

#### *3.4.1.6.6. Sarbanes oxley yasası*

Amerika Birleşik Devletleri'nde yönetişim alanında atılmış en önemli adım olan Sarbanes Oxley Yasası, 2002 yılında yürürlüğe girmiştir. Yasa düzenleyicileri olan ABD senatörü Paul Sarbanes ve ABD Temsilciler Meclisi üyesi Michael G. Oxley'in adlarıyla anılır. ABD başkanı George W. Bush'un ifadesiyle Amerikan başkanlarından Franklin D. Roosevelt döneminden bu yana işletme uygulamaları için düzenlenen en geniş kapsamlı reformdur (Cohen vd., 2008, s.758).

Sarbanes Oxley Yasasının amacı, halka açık işletmeler için yapılan finansal raporlamanın, bağımsız denetimin ve diğer muhasebe hizmetlerinin kalitesini ve şeffaflığını artırmak, muhasebe uygulamalarında standart bir çerçeve belirlenmesi sürecini hızlandırmak ve denetim şirketlerinin bağımsızlığını güçlendirmektir (Price, 2006, s.17). Yasanın temel amacı sermaye piyasalarında işletmelere ilişkin bilgilerin doğruluğunu ve güvenilirliğini artırarak yatırımcıları korumaktır. Yasa finansal raporlamanın ve denetimin kalitesini korumayı ve geliştirmeyi, yatırımcı ve çıkar

sahiplerinin özellikle büyük muhasebe skandalları sonucu sarsılan güvenlerini yeniden tesis etmeyi amaçlar (Marianne, 2006, s.4).

#### *3.4.1.6.7. Higgs raporu*

Higgs Raporu olarak anılan 'Bağımsız Yönetim Kurulu Üyelerinin Etkinliği ve Rolünün İncelenmesi' (Review of The Role and Effectiveness of Non-Executive Directors) isimli rapor 2003 yılında yayımlanmıştır. Daha önce yayımlanan Birleşik Kod'da yer alan öneriler üzerinde birçok değişiklik öngörmüş ve bunların neticesinde Birleşik Kod 2003 yılında yeniden düzenlenmiştir. Rapor özellikle bağımsız yönetim kurulu üyelerinin yönetişimin geliştirilmesindeki rolleri, işe alım süreçleri gibi konularda öneriler getirir. Bağımsız yönetim kurulu üyelerinin rolleri kısaca şöyle belirlenmiştir (Manifest, 2004, s.4):

- Kurumsal stratejiye katkı sağlamak,
- Yöneticilerin performanslarını izlemek,
- İç kontrolün etkinliğini geliştirmeye çalışmak,
- Yöneticilerin ücretlerini düzenlemek,
- Üst düzey yöneticilerin aday gösterilmesi ve azledilmesi ile ilgili işlemlerde yer almak.

#### *3.4.1.6.8. Myners raporu*

Hissedar Oy Haklarının Düzenlenmesi Çalışma Grubu başkanı Paul Myners daha çok kendi adıyla anılan 'Birleşik Krallık Hisselerine Oy Vermenin Önündeki Engellerin İncelenmesi' (Review of the İmpediments to Voting UK Shares) isimli raporunu 2004 yılında yayımlamıştır. Raporda sıralanan sorunların temelinde hesap verebilirlik mekanizmasının ve şeffaf bir sistemin oturtulamaması gibi yönetişim eksikliklerinin olduğu ve çok sayıda tarafın birbirinden farklı oy verme önceliklerine sahip olmasından kaynaklanan problemler olduğu vurgulanmaktadır. Raporun getirdiği en çarpıcı çözüm, oy verme işlemlerine herkes tarafından kolayca ulaşılabilirliğin sağlanması için elektronik oy verme sistemlerinin geliştirilmesidir. Raporda yönetişim için gerekli olan bileşenler şöyle tanımlanmıştır: etkili karar alma, açık amaçlar, ortakların sorumlulukları, şeffaflık ve raporlama. Rapor, işletmelerin faaliyetlerini yürüttükleri endüstrilerini

dikkate alarak kendi pratiklerini geliştirmeleri gerektiğini vurgular. 2008 yılında güncellenmiştir (Mallin, 2013, s.31).

#### *3.4.1.6.9. IIA- Yönetişim merkezi standartları*

Gelişmiş bir hisse senedi ve menkul kıymetler borsası olan hemen hemen her ülkede yönetişim için kodlar ve rehberler geliştirilmiştir. IIA, yönetişimle ve iç denetçilerin bu dönüşüme nasıl katkıda bulunmaları gerektiğiyle ilgili konularda öncü bir role sahiptir. Enstitü, Kennesaw Üniversitesi- Yönetişim Merkezi işbirliğiyle değişik üniversitelerden 20 profesör tarafından güçlü bir yönetişimin geliştirilmesi amacıyla hazırlanan yönetişim ilkelerinin takipçisi olunmasını desteklemektedir (Pickett, 2011, s. 32):

- "Sağlam bir yönetişim; yönetim kurulu, üst yönetim, iç denetim ve bağımsız denetim arasında güçlü bir etkileşimi gerektirir.
- Yönetim kurulu, amacının diğer paydaşların çıkarlarını dikkate alarak şirketin hissedarlarının çıkarlarını korumak olduğunun farkında olmalıdır.
- CEO'nun, işletme stratejisinin, risklerin ve iç kontrolün izlenmesi yönetim kurulunun başlıca sorumluluklarındandır. Yönetim kurulu üyeleri bu sorumluluğu uygun seviyede bir şüphecilikle üstlenmelidir.
- Borsa otoritesi işletmeye veya yönetime yönetici olarak hizmet etmekten başka hiçbir mesleki veya kişisel bağı olmayan birini bağımsız yönetim kurulu üyesi olarak atamalıdır.
- Yönetim kurulu üyelerinin büyük çoğunluğu yukardan aşağıya bir gözetimin teşvik edilmesi amacıyla bağımsız olmalıdır.
- Yöneticiler ilgili endüstri, şirket, fonksiyonel alan ve yönetişim uzmanlığına sahip olmalıdır. Tüm yöneticiler, gerekli uzmanlık düzeyini elde ettiklerinden ve bu düzeyi koruduklarından emin olmak için ayrıntılı oryantasyon ve sürekli eğitime tabi tutulmalıdır.
- Yönetim kurulu sık sık uzun süreli olarak toplanmalı ve görevlerini yerine getirmek için ihtiyaç duyduğu bilgiye ve personele erişmelidir.
- Yönetim kurulu başkanı ve CEO rolü birbirinden ayrılmalıdır.
- Vekâlet beyanları ve diğer yönetim kurulu iletişimleri yönetim kurulu faaliyetlerini ve işlemlerini şeffaf ve zamanında yansıtmalıdır.
- Yönetim kurulunun aday gösterme, ücret ve denetim komiteleri sadece bağımsız yönetim kurulu üyelerinden oluşmalıdır.
- Tüm halka açık şirketler, doğrudan denetim komitesine rapor veren etkili, tam zamanlı bir iç denetim birimine sahip olmalıdır.
- Mevcut finansal raporlama modeli, halka açık şirketler için giderek daha az uygun hale gelmektedir. Bilgi çağındaki şirketlerin maddi ve maddi olmayan kaynakları, riskleri ve performansları hakkındaki bilginin finansal tablo kullanıcılarına etkin ve verimli bir şekilde iletilebilmesi için

kullanılan model değiştirilmeli veya geliştirilmelidir. Yeni model en kısa zamanda geliştirilmeli ve hayata geçirilmelidir.

- Mali tablolar ve destekleyici açıklamalar ekonomik unsurları yansıtmalı ve maksimum bilgilendirici olma ve şeffaflık amacıyla hazırlanmalıdır. Güvenilir finansal raporlama için yönetimin dürüstlüğü ve güçlü kontrol ortamı kritik önem taşır.
- Denetim komitesi finansal, denetim ve endüstri özelinde uzmanlığa sahip bağımsız üyelerden oluşmalıdır. Bu üyelerin, finansal raporlama sürecinin özenle gözetimini sağlamak amacıyla gerekli olan otorite, yetki ve kaynakları olmalıdır. Yönetim kurulu, denetim komitesi üyelerinin hisse senedi/opsiyon varlıklarının risklerini göz önünde bulundurmalı ve denetim komitesi üyelerinin kazançlarını üstlendikleri görevler ve üyelerin karşılaştıkları risklere göre uygun bir seviyeye getirmelidir. Denetim komitesi bağımsız denetçiyi seçmeli, bağımsız denetçi ve iç denetçinin performansını değerlendirmeli, denetim ücretini onaylamalıdır.
- Hileli finansal raporlama davalarında işletme yönetimi katı cezai yaptırımlarla karşı karşıya kalmalıdır. Yönetim kurulu, üst yönetim ve denetçiler hile riski değerlendirmeleri yapmalıdır.
- Denetim firmaları öncelikle yüksek kaliteli denetim ve güvence hizmetleri sunmaya odaklanmalı ve denetim müşterileri için hiçbir danışmanlık faaliyeti yapmamalıdır. Denetim ücreti işin kapsamını ve riskleri yansıtmalıdır.
- Bağımsız denetçiler muhasebe işini rekabet edilmesi gereken bir iş olarak değil kamu yararına odaklanan asil bir meslek olarak görmelidir."

#### *3.4.1.7. Yönetişimde iç denetimin sorumlulukları*

Yönetişim işletmenin paydaşlarının temsilcileri olarak yönetim tarafından idare edilen kontrol süreçlerinde ve riskin izlenmesinde kullanılan yordamlar ve faaliyetlerden oluşur. Etkili yönetişim, yönetime doğru raporlama yapılmasına (iç kontrollerin ve finansal sonuçların raporlanması gibi) ve etkili iç kontrollerin oluşturulmasına yardımcı olur. Yönetişimin dört köşe taşı olarak kabul edilen denetim komitesi, üst yönetim, bağımsız denetçiler ve iç denetim birimi işletme paydaşlarının en başta gelen temsilcileri olarak görülürler (Gramling vd., 2004, s. 196).[7]

Yönetişim, risk yönetimi ve iç kontrol alanında yapılan düzenlemelere bakıldığında, yeni yaklaşım ve ihtiyaçların gündemi yönlendirdiği ve bu bağlamda yönetim kurulu, denetim komitesi ve iç denetimin sorumluluklarının önem kazandığı anlaşılmaktadır. Yönetişim tanımı, ilkeleri ve ilişkileriyle beraber değerlendirildiğinde, işletmenin tüm paydaşlarının menfaatlerinin korunduğu bir güvence yaklaşımı ortaya çıkmaktadır. Bu güvencenin sigortası iç denetimdir. Düzenleme, ilke ve standartlar iç

[7] Tabi ki diğer kesimlerin ve kurumların (kurumsal yatırımcılar, yasal sistem, düzenleyici kurumlar gibi) yönetişim üzerindeki endirekt rolleri yadsınamaz.

denetimin rolünü kritik hale getirmiştir. Özellikle SPK ve BDDK tarafından yapılan düzenlemelerde iç denetimle ilgili ayrıntılı maddeler yer almaktadır. Bu düzenlemeler yönetim kurulu, denetim komitesi, iç denetim ve bağımsız denetime yönetişim alanında yeni sorumluluklar yüklemiştir. İç denetime yüklenen sorumluluklar güncel iç denetim tanımında da kendisine yer bulmuştur (Uzun, 2010, s. 1).

Güncel tanımına bakıldığında iç denetimin rolünün değiştiği ve sorumluluklarının arttığı görülmektedir. Dünün işlem ve hata odaklı yaklaşımı yerini süreç odaklı işin etkinliğinin artırılmasına yönelik bir stratejik akıl ortaklığına bırakmıştır. İşletme içinde tarafsızlık ve bağımsızlık özelliklerine sahip olan iç denetimin yönetişim rolü değerlendirildiğinde, süreçlerin iyileştirilmesi, insan kaynağının gelişimi, kurumsal performans ve verimlilik yönetimi, iç iletişim, iyi uygulamaların paylaşılması ve katma değer yaratılmasında sorumluluklar üstlenildiği anlaşılmaktadır (Uzun, 2010, s. 2).

Yönetişim ve iç denetim birbirleriyle etkileşim içinde olan ve birbirlerini tamamlayan iki unsurdur. İşletmede etkin bir yönetişim anlayışının olmaması denetim mekanizmasında eksikliklerin ortaya çıkmasına yol açar. Ancak iyi tanımlanmış etkin işleyen bir mekanizma, denetçilerin görevlerini yapmalarını kolaylaştıracak ve kaynakların verimli kullanılmasını sağlayacaktır. Ayrıca iç denetim ve yönetimi birbirilerine yakınlaştıracak ve uyumlu çalışmalarını kolaylaştıracaktır (Alparslan, 2000, s. 94).

Yönetişim geliştirilirken iç denetimden yararlanılması hata, hile ve suiistimalleri önleyeceğinden tüm menfaat sahipleri arasında dengenin kurulması açısından güvence sağlar. İyi bir yönetişimin sağlanabilmesi için öncelikle iyi işleyen bir iç denetim faaliyetine ihtiyaç vardır. Bağımsız denetim, tek başına iyi yönetişim için yeterli olmayacaktır (Küpçü, 2011, s. 107).

İç denetim birimi işletme içinde stratejik bir pozisyona sahip olursa, işletme performansının geliştirilmesine katkı sağlar. Stratejik bir pozisyona iç denetim biriminin misyonuna ve rolüne geniş bir yönetişim çerçevesinin içinde yer verilerek ve etkin bir iletişim sağlanarak ulaşılabilir. Ayrıca, iç denetimin yapısı nesnelliği, tutarlılığı ve iş anlayışını geliştirmelidir. İç denetim uygun başarı ölçütleri tarafından belirlendiği şekilde işletmeye değer katmalıdır. İç denetim, yönetişime katılan tüm karar faktörlerinden bağımsız olmalıdır. İç denetim fonksiyonu denetlenen faaliyetlerden ve günlük iş süreçlerinden bağımsız olmalı ve işletmenin tüm birimlerinde, bağlı işletmelerinde ve süreçlerinde atanmaksızın kendi inisiyatifiyle hareket edebilmelidir (Florea, 2013, s. 81).

İç denetimin benimsediği yapı ve raporlama hatları bağımsızlık, nesnellik, tutarlılık ve iş anlayışını geliştirmelidir. Bu ancak iç denetim biriminin işletme içindeki diğer birimlerden bağımsız şekilde çalışabilmesine izin veren bir örgütsel yapıyla yönetim kurulu/denetim komitesine açık bir raporlama hattıyla ulaşılması sayesinde başarılabilir. IIA işletmenin seçtiği raporlama ilişkilerine bakılmaksızın, iç denetim biriminin etkinliği ve bağımsızlığına olanak tanıyacak ve raporlama hatlarının desteklenmesini sağlayacak anahtar önlemleri tavsiye eder. İç denetim birimi yönetmeliği temel faaliyetlerinin yanı sıra hem idari hem de fonksiyonel raporlama hatlarını açıkça ifade etmelidir. İç denetim biriminin denetim komitesine doğrudan raporlama yapmasının faydaları şunlardır (Florea, 2013, s. 82):

- Kapsam sınırlaması korkusu olmaksızın örneğin finans birimiyle ilişkiler yürüterek diğer birimlerden üstün bir konum elde edilir.
- Yönetim kurulu ve denetim komitesi, iç kontrol ve risk yönetimine ilişkin elde ettikleri bilginin özellikle yönetim tarafından müdahale edilmeden direkt raporlandığı için gerçeği yansıttığından emin olurlar.
- İç denetim biriminin bağımsızlığı kesinleşir.
- İç denetim biriminin finansmanı, bütçelemenin normal süreci dışındadır, böylelikle, kaynakların yönetim kurulu / denetim komitesi tarafından değerlendirildiği şekilde kuruluşun güvence ihtiyaçları tarafından tahsis edilmesine izin verilmektedir.
- Yönetim kuruluna / denetim komitesine, yönetim kurulunun bir sorumluluğu olan iç kontrole katkı sağlayan ve aynı zamanda onun bir parçası olan iç denetimin doğrudan analiz edilmesi ve değerlendirilmesi fırsatını sunar.
- Yönetim kurulunu / denetim komitesini üst yönetim ve paydaşlarla uğraşırken işletme ve risk yaklaşımı bilgisiyle destekler.

Blue Ribbon Komitesi, denetim komitesi ve iç denetimi de kapsayacak biçimde yönetişimin gözetim sorumluluklarına ilişkin bazı sonuçları göz önüne sermiştir (Rezaee vd, 2003, s. 531):

Kaliteli finansal raporlama ancak açık ve samimi bir iletişim ve işletmenin yönetim kurulu, denetim komitesi, üst yönetimi, iç denetçileri ve dış denetçileri arasında yakın çalışma ilişkileri yoluyla elde edilebilir.

1. Halka açık şirketlerin finansal raporlama sürecinde yönetişimin gözetimini güçlendirmesi, finansal tablo hilelerini azaltır.

2. Finansal tablo hileleri yatırımcı güvenine zarar verirken, finansal raporların doğruluğu, kalitesi ve şeffaflığı sermaye piyasalarında bu güveni geliştirir.

İşletmenin amaçları doğrultusunda faaliyetlerini kişilerin varlığına bağlı olmadan sürdürebilmesini sağlayan bir yönetim ve örgüt yapısı oluşturması anlamına gelen kurumsallaşmanın en önemli göstergesi işletmede iç denetim faaliyetlerinin yapılmasıdır. Eğer işletmede düzgünce organize edilmiş ve çağdaş normlarla hareket eden bir iç denetim birimi oluşturulmuşsa, bu durum kurumsallaşma ve yönetişimin varlığının önemli bir göstergesidir. Ayrıca işletmenin yönetişimi geliştirmesi, iç denetimden elde edilen faydaları arttırır. Bu anlamda yönetişim iç denetimi, iç denetim de yönetişimi gerekli kılmaktadır. Karşılıklı bu ilişki, yönetişim ilkelerinin her biri açısından açıklanabilir. İç denetim, faaliyetleri bir bütün olarak ve tüm detayları ile incelendiğinde bu konuda yapılan raporlamalarda (Türedi, Karakaya & İldem, 2015, s. 68);

- "İşletme üst yönetiminin politikaları ve talimatları doğrultusunda gerçekleşen ekonomik faaliyetlerin, etraflı bir şekilde değerlendirildiği görülmektedir. Bu değerlendirmeler yönetim kurulunun hesap verebilmesini kolaylaştırır.
- İşletme pay sahipleri, işletme çalışanları ve diğer paydaşların hakları ve sorumlulukları işletmenin faaliyetleri kapsamında değerlendirildiğinden muhtemel çıkar çatışmaları ve haksızlıklar görülebilmektedir. Bu değerlendirmelerden hareket edilerek zedelenen eşitlik ve adalet ilkeleri onarılmaya çalışılır.
- İşletmenin karşı karşıya kaldığı riskler ve bu risklerin yol açtığı olumsuz sonuçlar etraflıca değerlendirilmektedir. Bu değerlendirmeler rehber alınarak sorumlu olanlar hakkında işlem yapılabilir.
- İşletmenin mali ve mali olmayan tüm faaliyetleri, taraflarca anlaşılabilecek şekilde, zamanında, tam ve doğru olarak aktarıldığından işletme faaliyetlerinde şeffaflık sağlanmış olur."

Uluslararası İç Denetim Standartları da, iç denetçilerin yönetişim hakkındaki rol ve sorumluluklarına değinmiştir. Performans Standardı 2130, iç denetim faaliyetinin yönetişim süreçlerinin geliştirilmesi için uygun tavsiyeleri getirmesi gerektiğini ve süreci değerlendirmesi gerektiğini ifade eder ve aşağıdaki amaçlara ulaşılması için iç denetçilere sorumluluklar yükler (IIA, 2010a, s. 17):

- Kurum içinde gerekli etik ve diğer değerlerin geliştirilmesi,
- Etkili bir kurumsal performans yönetimi ve hesap verebilirlik,
- Risk ve kontrol bilgilerinin kurumun gerekli alanlarına etkili bir şekilde iletilmesi,

- Yönetim kurulunun, denetim komitesinin, iç ve dış denetçilerin ve üst yönetimin faaliyetleri arasında eşgüdüm sağlamak ve bunlar arasında gerekli bilgilerin etkili bir şekilde iletilmesini sağlamak.

Son on yılda, yönetişimin yeni yaklaşımları, yönetim kurulunun işletmelerin iç kontrol çerçevesinin etkinliğini sağlamaya yönelik sorumluluğunu tamamen doğrulamıştır. Bu teoriler, iç denetimin, iç kontrollerin yeterli gözetimini sağlamada ve bir kuruluşun yönetişim çerçevesinin ayrılmaz bir parçasını oluşturmasında yönetim kurulunun desteklenmesinde oynayabileceği kilit rolü vurgulamaktadır. İç denetimin kilit sorumluluğu aşağıda sıralanan yönetişim sorumluluklarını yerine getirerek destek sağlamaktır (Florea, 2013, s. 80):

- Organizasyon kültürünün özellikle de yönetim tarzının incelenmesi,
- Mevcut risk ve iç kontrol çerçevesinin objektif bir değerlendirmesinin yapılması,
- İşletme süreçlerinin ve ilişkili kontrollerin sistematik analizinin yapılması,
- Mevcut değerlerin ve varlıkların yeniden incelenmesi,
- Büyük yolsuzluk ve usulsüzlüklerle ilgili bilgi kaynağı olunması,
- Kabul edilemeyen riskleri de kapsayacak şekilde endişe duyulan diğer alanlarla ilgili özel amaçlı yeniden incelemelerin yapılması,
- Uygunluk çerçevesi ve özel uygunluk sorunlarının yeniden incelenmesi,
- Operasyonel ve finansal performansın yeniden incelenmesi,
- Kaynakların daha etkili ve verimli kullanılması amacıyla tavsiyelerin geliştirilmesi,
- Kurumsal amaçlara ulaşılıp ulaşılmadığının değerlendirilmesi
- Etik ve davranış kodlarıyla işletmenin değerlerine bağlılık konusunda geri dönüt verilmesi.

Sermaye Piyasası Kurulu tarafından yayınlanan yönetişim ilkeleri gereğince işletme yönetim kurullarının belirlenmiş sorumluluklarını yerine getirmelerine yardımcı olmak amacıyla, nihai sorumluluk işletme yönetim kurulunda kalmak üzere, bağımsız yönetim kurulu üyeleri arasından seçilerek oluşturulacak komitelere yer verilmektedir. Bu komitelerin en önemlilerinden biri denetim komitesidir. Denetim komitesi, iç denetimin güvence ve danışmanlık fonksiyonlarını bağımsız ve tarafsız olarak yerine getirmesi için oluşturulmuş bir komitedir. Yönetişim içerisinde etkin olarak işleyen bir denetim komitesinin bulunması iç denetim faaliyetlerinin kalitesini ve etkinliğini

artıracağı gibi aynı zamanda paydaşların haklarının korunması için oluşturulan yönetişimin önemli bir parçasını oluşturacaktır (Türedi, Karakaya ve İldem, 2015, s. 69).

Denetim komitesi, yönetim kurulu adına, iç ve bağımsız denetimin uygulama etkinliğini ve katma değerini; muhasebe, finansal raporlama ve iç kontrollerin yeterliliğini ve işleyişini gözetimle görevlidir. Bu işleviyle yönetim kuruluna güvence sağlar. Denetim komitesinin yapısı komitenin etkinliğini belirleyen temel faktörlerin başında gelir. Denetim komitesinin üyeleri bağımsız yönetim kurulu üyelerinin arasından seçilir (TÜSİAD, 2012, s.13). Komite yönetişim açısından önemli bir role sahiptir ve şirket içerisinde kaliteli ve güvenilir finansal raporlama ve kontrol sistemlerinin sağlanmasının yanı sıra risklerin tespiti ve yönetilmesinde önemli bir rol üstlenir (Hermanson & Rittenberg, 2003, s.50). Denetim komitesinin yönetişim içerisinde rolü genel olarak şu şekilde özetlenebilir.

- ***Finansal Raporlama Sürecinin İzlenmesi***: Denetim komitesinin esas sorumluluğu işletmenin güvenilir finansal raporlama gerçekleştirme amacına destek olmak için finansal raporlama sürecinin izlenmesidir. Komitenin bu alandaki sorumlulukları; işletmenin kazanç kalitesinin değerlendirilmesi, finansal raporların ve açıklamaların incelenmesi ve hileli finansal raporlama riskinin değerlendirilmesidir (Hermanson & Rittenberg, 2003, s.50).
- ***Risk Yönetimi ve İç Kontrol Sistemleri***: İşletmelerin faaliyetlerini sürdürürken maruz kaldıkları çeşitli riskleri yönetmek denetim komitesinin sorumluluğunda olmasa da, özellikle finansal raporlama, mevzuata uygunluk, hile ve bilgi sistemleri alanlarındaki risklerin değerlendirilme sürecinin gözetilmesi denetim komitelerinin görev alanlarına girmektedir. Öte yandan, denetim komitesi şirketin iç kontrol yapısının yeterliliğini ve etkinliğini değerlendirmek zorundadır. İç kontroller, maruz kalınan riskleri kabul edilebilir seviyelere indirebilmek amacı ile oluşturulduğundan etkin bir iç kontrol sisteminin varlığı, başarılı bir risk yönetim sürecinin ön koşullarından biridir (TÜSİAD, 2012,15-16).
- ***İç ve Bağımsız Denetim Süreçlerinin İzlenmesi***: Denetim komitesinin iç ve bağımsız denetime yönelik sorumlulukları da vardır. İç denetim süreci bakımından denetim komitesi; iç denetim planının, yordamlarının, kapsamının ve iç denetim sonuçlarının gözden geçirilmesinden sorumludur (Reeaze & Riley, 2002, s. 167). Diğer bir ifadeyle iç denetim sürecine ait faaliyetlerin gözden geçirilmesi denetim komitesinin görevlerinden biridir. Denetim komitesinin, bağımsız denetime yönelik

sorumlulukları da iç denetime benzerdir. Bağımsız denetçilerin göreve getirilmesi ve görevden alınması, denetçilerin bağımsızlıklarının değerlendirilmesi, bağımsız denetim raporunun gözden geçirilmesi ile yönetimin iç kontrol ile ilgili değerlendirmelerine yönelik bağımsız denetçilerin hazırladıkları raporların değerlendirilmesi denetim komitesinin sorumlulukları arasındadır (Carcello & Neal, 2000, s. 455).

Denetim komitesinin görev ve fonksiyonları, iş çevresindeki değişikliklere yanıt olarak gelişmiştir. Denetim komitesinin özetle başlıca sorumlulukları yönetim kuruluna aşağıda sıralanan konularda destek sağlamaktır (Soltani, 2007, s. 95):

- İşletmenin finansal tablolarının doğruluğu;
- Bağımsız denetçilerin dürüstlüğü, bağımsızlığı, performansı ve özellikleri;
- İşletmenin iç denetim biriminin performansı;
- İşletmenin iç kontrol sisteminin uygunluğu;
- Davranış kodlarına ve yasal düzenlemelere uygunluğun izlenmesi.

Denetim komitesinin diğer önemli fonksiyonları şunlardır (Soltani, 2007, s. 95):

- Önemli muhasebe ve raporlama sorunlarının incelenmesi ve finansal tablolar üzerindeki etkilerinin anlaşılması;
- Periyodik toplantılar yaparak yönetim kurulu, finansal yönetim, iç denetçiler ve bağımsız denetçiler arasında doğrudan bir raporlama iletişiminin kurulması ve devam ettirilmesi;
- İşletmenin iç kontrolünün etkinliğinin, iç denetimin kapsamının ve bağımsız denetçilerin finansal raporlama üzerindeki iç kontrol incelemelerinin değerlendirilmesi;
- Yasalara ve düzenlemelere uygunluk, etik, çıkar çatışması ve hile araştırmalarıyla ilgili işletme politikaları için işletmenin iç kontrol sisteminin etkinliğinin incelenmesi.

Denetim komitesi, görevlerini yerine getirirken, yürürlükteki kanunlar, düzenlemeler ve standartlara uygun olarak şirketin yıllık finansal tablolarına eklenecek bir rapor hazırlamalı ve genel kurula sunmalıdır. Yönetim kurulunun performansını değerlendirirken denetim komitesinin sorumluluğu, sadece yöneticilerin yasal gerekliliklerini yerine getirip getirmedikleri değil, daha da önemlisi, etik ilkelere olan saygı ve bunu uygulamaya nasıl yansıttıklarıdır.

Denetim komitesi yatırımcılar ve iç denetçiler için hayati derecede önemlidir. Denetim komitesi sayesinde yatırımcılar yönetişim hakkında güvence elde ederler. İç denetçiler ise bağımsızlıklarını güçlendirirler. İç denetçiler işletme içinde üst düzey çalışanlara rapor sunarken, aynı zamanda kendilerinden yönetimin davranışlarını ve etkinliğini nesnel bir şekilde değerlendirmeleri beklenmektedir. Bu sorunun tek tatmin edici rasyonel çözümü, iç denetimin öncelikli olarak üst yönetim yerine doğrudan yönetim kurulu ve denetim komitesine raporlama yapabilmesidir (Florea, 2013, s. 81).

Üstlendiği sorumlulukları hakkıyla yerine getirmesi için denetim komitesinin de bağımsız olması gereklidir. Komitenin bağımsızlığının sağlanabilmesi için, üyelerinin hiçbir etki altında kalmadan, kimseden çekinmeden ve çıkar çatışmasına girmeden karar alabilmesi ve görüş bildirebilmesi gerekir. Bunu sağlayabilmek için, komite üyeleri işletme faaliyetleriyle ilgili icrai sorumluluklar almamalı, özellikle yönetimden tamamen bağımsız olmalıdırlar. Etkin bir denetim komitesinin önde gelen koşulu, komite üyelerinin yönetimden bağımsız hareket edebilecek özelliklere sahip olmasıdır. Komite üyelerinin bağımsızlıklarının korunması için nitelikli pay sahibi ortak olmamaları, icrai görev üstlenmemeleri, hâkim ortak ya da icrai görev üstlenen yöneticinin eşi veya yakın akrabası olmamaları ve kendilerine karlılığa bağlı bir kazanç sağlanmaması gereklidir (Yenigün, 2008, s. 78-79).

### 3.4.2. Kurumsal Risk Yönetimi

Birçok işletmede risk yönetimi, yönetişim sürecinin ayrılmaz bir parçası haline gelmiştir. Etkili risk yönetiminin etkin yönetişime ulaşmayı sağladığını vurgulayan yönetişim, risk ve uygunluk (YRU) kavramı giderek daha fazla popülerlik kazanmaktadır. İşletmede iç rehberlere ve dış düzenlemelere uyum sağlama başarısını gösteren etkili yönetişim yapısının oluşturulması için, işletmenin risk değerlendirme süreçlerinin kalitesinin ve bu süreçlerin iç koordinasyonunun büyük önem taşıdığı anlaşılmıştır (Schneider vd., 2012, s. 27).

YRU süreçlerinin bir parçası olarak iç denetim, iç ve dış değişikliklerin kuruluşun performansını olumsuz olarak etkileme potansiyelini değerlendirmelidir. İç denetçilerin yönetimin risk yönetimi süreçlerinin yeterliliğini değerlendirmesi gereklidir. Risk yönetimi süreçlerinin yeterliliğini ve işletmenin varlıklarını, itibarını ve devam eden faaliyetlerini etkileyebilecek risklere gerektiği gibi tepki verip veremediği incelenmelidir. IIA mesleki standartları, risk yönetiminin üst yönetimin sorumluluğunda olduğunu

belirtmektedir. Aynı zamanda, iç denetim, risklerin gerektiği gibi ele alınması için yönetim tarafından geliştirilen metodolojilerin ve kontrollerin değerlendirilmesi ve iyileştirilmesinde rol oynar. İç denetçiler özellikle yönetimin risk toleransı seviyeleri oluşturduğuna ve risk süreçlerini ve etkinliklerini yeniden değerlendirmek için kontrollerin sürekli olarak izlediğine dair güvence vermelidir. İç denetim yönetişim süreçlerinin, riskleri doğru bir şekilde tanımladığına, değerlendirdiğine ve yönettiğine dair güvence sağlamalıdır (Coderre, 2009, s. 99).

IIA KRY'ni risk uygulayıcılarının işletmeleri için KRY uygulamalarına rehberlik ettiği ve iç denetçilerin genellikle bu uygulamaları değerlendirdiği bir süreç olarak tanımlar. Bununla birlikte, risk yöneticileri ve iç denetçiler kurumsal risk yönetimini benzer şekilde düşünmelidirler. İşletmede hem risk yönetiminden sorumlu olan yöneticiler hem de iç denetim uzmanları, ISO 31000 spesifik risk yönetim standartlarını ve IIA Uluslararası Mesleki Uygulama Çerçevesi, COSO KRY Çerçevesi ve Açık Uygunluk ve Etik Grubunun YRU Modeli gibi rehber dokümanları işletmelerinin risk yönetimine katkı sağlamak ve söz konusu faaliyetlerin iç denetim işlevini yerine getirmek amacıyla kullanabilirler. Bir risk yönetim standardı ya da rehber doküman kullanmak ve ilgili ilkeleri kuruluşun kültürü ve süreçlerine uyarlamak etkin risk yönetimi için bir anahtardır (RIMS, 2012, s. 5).

#### *3.4.2.1. Risk ve risk yönetimi*

COSO'nun ifadesiyle risk, bir olayın ortaya çıkma ve kurumun amaçlarına ulaşma başarısını olumsuz etkileme olasılığıdır. Uluslararası Standardizasyon Örgütü (ISO), riski, belirsizliğin amaçlar üzerindeki etkisi olarak tanımlamıştır (Parkinson, 2018, s. 9). Risk, birçok olumsuz sonuç doğurabilen, önemli bir etmendir. İstenilen şeylerin elde edilmesi ya da istenmeyen şeylerin ortaya çıkmasını engellemek için risklerin iyi yönetilmesi gerekir. Risk yönetimi ise işletmenin amaçlarına ulaşmasını engelleyecek risklerin tespit edilmesi, azaltılması ve başarıya ulaşılmasını sağlayacak fırsatların ortaya çıkarılarak kullanılması sürecidir (Reding vd., 2013, s. 4-3).

Risk yönetimi, her türlü risklerin tanımlanması, ölçülmesi ve giderilmesini kapsayan sistematik bir yönetim uygulamasıdır. Belirsizlikleri ve belirsizliğin yaratacağı olumsuz etkileri daha kabul edilebilir bir düzeye indirgemeyi sağlayan bir disiplindir. Problem haline gelmeden, yani tehlikeye dönüşmeden önce, risklerin belirlenmesini, risklerin oluşma olasılığını ve etkisini en aza indirgeyen faaliyetlerin planlanmasını ve

yürütülmesini kapsar. Problemlerin oluşmadan önlenmesini sağlayan proaktif bir yaklaşımdır (Fıkırkoca, 2003, s. 14).

YRU kısaltmasındaki R, risk yönetimini simgeler. OCEG'in yaptığı tanıma göre risk, amaçlara ulaşma üzerinde etkisi olacak, daha da önemlisi olumsuz bir etkiye sebep olacak şeylerin gerçekleşme olasılığının ölçüsüdür. Risk yönetimi ise, bir organizasyonun riskleri tanımlayan, değerlendiren, analiz eden, optimize eden, izleyen, düzelten veya riske ilişkin iletişim kurarken ve riske bağlı karar alırken riski paydaşlara transfer eden süreçlerin ve yapıların sistematik bir şekilde uygulanmasıdır. Risk yönetiminin temel amacı, risklerin olumsuz etkilerini yönetirken potansiyel fırsatların farkında olmaktır (OCEG, 2009, s. 9).

Risk yönetimi değer yaratmalı ve örgütsel süreçlerin tamamlayıcı unsuru olmalıdır. Karar verme süreçlerinin bir parçası olmalıdır ve bir işletmenin karşılaştığı belirsizlikleri açıkça gidermek için sistematik ve yapılandırılmış bir şekilde işletmeye özgü olarak düzenlenmelidir. Ayrıca, risk yönetimi süreci, sürekli iyileşme ve gelişme yeteneğiyle değişime cevap verebilmeli ve dinamik olmalıdır (Moeller, 2011, s. 26).

Bir işletmede iyi iç kontrol yapısı etkili risk yönetimi için olmazsa olmazdır. İç kontroller çeşitli alanlarda işletme faaliyetlerinin içerisindedir. Örneğin, işletmeye dışardan bir mal satın alırken görevler açık şekilde ayrılmalıdır. Malı teslim alanla ödeme belgesini onaylayan aynı kişi olmamalıdır. Böylece, iyi tanımlanmış iç kontroller sayesinde, benzer durumlarla ilişkili birçok kişi, başka bir kişinin işini bağımsız bir şekilde kontrol etmek için iyi bir pozisyona sahip olacaktır (Moeller, 2011, s. 1).

#### *3.4.2.2. Kurumsal risk yönetimi kavramı*

Kurumsal risk yönetiminin başlangıç noktası, tüm işletmelerin belirsizlik yaratan faktörlerle mücadele etmek zorunda olmasıdır. Belirsizlik, işletme için hem değer yaratan olanakları hem de değer artırılmasını engelleyen riskleri ortaya çıkaran bir unsurdur. KRY, işletmenin üst yönetimi ve yönetim kurulu dâhil olmak üzere tüm işletme çalışanlarından etkilenen, işletmeyi etkileyebilecek tüm belirsizliklerin tespit edilmesi ve işletme amaçlarıyla uyumlu kalınması konusunda makul güvence sağlayan bir süreçtir. KRY işletmenin karşılaştığı tüm belirsizliklerin etkili bir şekilde yönetilmesi için gerekli olan yetenekleri geliştirir. KRY risklerin belirlenmesi, ölçülmesi, önem sırasına göre düzenlenmesi ve oluşan risklere karşı önemli amaçları, ilgili projeleri ve günlük faaliyetleri dikkate alarak gerekli tepkinin verilmesinde, işletme misyonu ve büyüklüğü

fark etmeksizin, tüm organizasyonlara sistematik şekilde katkı sağlayan bir yaklaşımdır (PWC, 2006, s. 6).

KRY, bir işletmenin kurumsal amaçlarından herhangi birine müdahale edebilecek riski tanımlayan, değerlendiren ve yöneten bütüncül bir süreçtir. Daha basit bir ifadeyle, bir işletmeyi makul bir olasılıkla önemli derecede etkileyebilecek tüm risklerle uğraşan sistematik bir yaklaşımdır. Bu potansiyel ortaya çıktığında, işletme yönetimi, riskleri analiz etmeli ve bunları yönetmek için ne yapacağını belirlemelidir. Söz konusu faaliyetler, riskin işletmenin risk toleransına dâhil edilmesi sonrasında riskin azaltılması, ortadan kaldırılması ya da hiçbir eylemde bulunulmaması seçeneklerini kapsar (Steinberg, 2011, s. 81).

IIA, İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol adlı pozisyon raporunda kurumsal risk yönetimini (KRY) şöyle tanımlamıştır (IIA, 2004, s. 3):

"*Kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için kurum çapında uygulanan, özel yapılandırılmış, istikrarlı, tutarlı ve kesintisiz bir süreçtir.*"

KRY kapsamındaki faaliyetler şöyle sıralanabilir:

- İşletmenin amaçlarını açıkça belirlemek ve işletme içinde iletişim kurmak;
- İşletmenin risk iştahının belirlenmesi;
- Bir risk yönetimi çerçevesini de kapsayacak şekilde uygun iç ortamın geliştirilmesi;
- Amaçlara ulaşılmasının önündeki potansiyel tehlikelerin tanımlanması;
- Risklere verilecek yanıtların seçilmesi ve uygulanması;
- Riske yanıt verecek kontrol ve diğer faaliyetlerin üstlenilmesi;
- İşletme içindeki tüm seviyelere tutarlı bir şekilde riske ilişkin bilginin iletilmesi;
- Risk yönetim süreçleri ve çıktılarının merkezi olarak izlenmesi ve koordine edilmesi;
- Risk yönetiminin etkinliğine güvence sağlanması.

2004 yılında COSO tarafından riskin belirlenmesi, değerlendirilmesi ve yönetilmesi konusunda işletmelere katkı sağlamak amacıyla yayımlanan Kurumsal Risk Yönetimi – Bütünleşik Çerçevede KRY şöyle tanımlanmıştır (COSO, 2004, s. 4):

"*KRY işletmenin yönetim kurulu, üst yönetimi ve diğer çalışanları tarafından etkilenen; stratejilerin geliştirilmesi ve işletme çapında uygulanması, işletmeyi etkileme olasılığı olan olayların belirlenmesi, risklerin işletmenin risk iştahı kapsamında*

*yönetilmesi ve işletme amaçlarına ulaşılmasına yönelik makul güvence sağlayan bir süreçtir.*"

COSO bu tanım içerisinde yer alan temel kavramları açıklamıştır (Reding vd., 2013, s. 4-4; Beasley, Frigo & Litman, 2007, s. 26; COSO, 2004, s. 4).

- İşletme çapında sürekli devam eden bir süreçtir.
- İşletmenin tüm seviyelerinde yer alan çalışanlar tarafından etkilenir.
- İşletme stratejilerinin düzenlenmesinde uygulanır.
- İşletme genelinde bütün seviye ve birimlerde uygulanır.
- İşletme seviyesinde bir risk portföyü oluşturulmasına odaklanır.
- Eğer meydana gelirse işletmeyi etkileyebilecek potansiyel olayların belirlenmesi ve riskin bir işletmenin kabul etmeye ve üstlenmeye istekli olduğu risk seviyesi anlamına gelen risk iştahı içerisinde yönetilmesi için tasarlanır.
- İşletmenin yönetim kurulu ve üst yönetimine makul seviyede güvence sağlayabilir.
- Birbirinden ayrı fakat örtüşen bir veya daha fazla kategoride amaçlara ulaşılması için uygulanır.

COSO, PWC işbirliği ile Kurumsal Risk Yönetimi – Strateji ve Performansla Riskin Düzenlenmesi adlı yeni bir KRY Çerçevesi hazırlamıştır. COSO'nun 2016'da yayımladığı yeni çerçevede yer alan güncel tanım, kurumsal risk yönetimiyle stratejilerin geliştirilmesi ve uygulama süreci arasındaki ilişkiye vurgu yapar ve kullanıcıların KRY konusunda işletme stratejilerine odaklanmaları gerektiğini vurgular (COSO, 2016, s. 10):

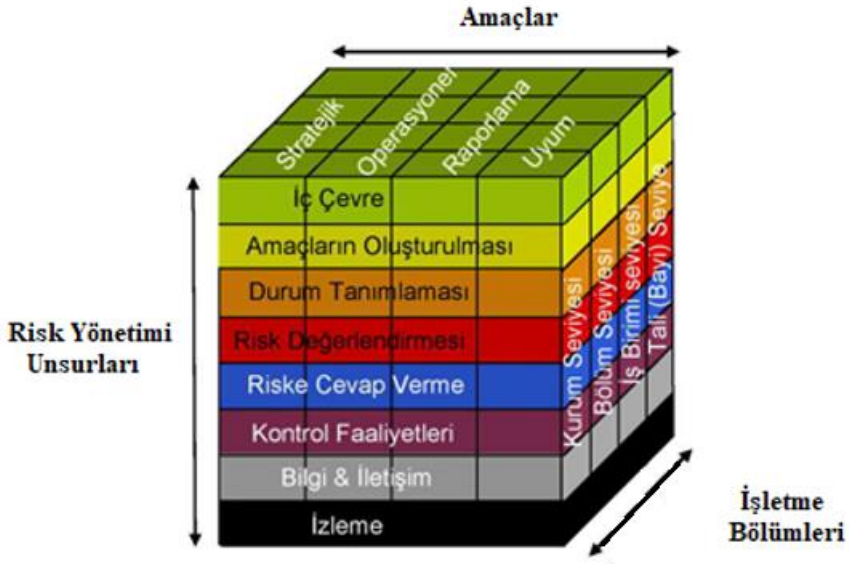
"*Kurumsal Risk Yönetimi, değerin anlaşılması, korunması ve yaratılması sırasında riskin yönetilmesi için işletmelerin güvendiği stratejinin düzenlenmesi ve uygulanmasıyla bütünleştirilmiş kültür, yetenek ve pratiklerdir*."

COSO'nun yayımladığı güncel çerçeve, risk yönetiminde aşağıda sıralanan eylemlere odaklanılmasını vurgular (COSO, 2016, s. 10):

- Kültür ve yeteneklerin anlaşılması;
- Strateji düzenleme ve yürütülmesi süreciyle bütünleşme;
- Strateji ve işletme amaçları için riskin yönetilmesi;
- Değer yaratma, koruma ve değerin anlaşılması aşamalarının birlikte ele alınması.

### *3.4.2.3. Kurumsal risk yönetiminin unsurları*

2004 yılında yayımlanan COSO KRY çerçevesine göre KRY birbiriyle ilişkili sekiz unsurdan oluşur. Bu bileşenler üst yönetimin işletmeyi yönetme biçiminden türetilmiştir ve yönetim süreçleriyle bütünleşiktir (Bkz. Şekil 3.5).




**Şekil 3.5.** *COSO KRY Küpü (COSO, 2004)*

#### *3.4.2.3.1. İç çevre*

Bu bileşen işletmenin risk alma yaklaşımını yansıtır ve işletmenin bütün çalışanlarının risk ve kontrol bilincini etkilemesine katkı sağlar. Üst yönetim bir rehber olarak, işletmenin tüm çalışanlarının riske yönelik tutumlarının temelini oluşturmaktan sorumludur. Bu bakımdan COSO kontrol ortamıyla birtakım benzerlikler taşır (Moeller, 2004, 235).

İç çevre, işletmenin yönetim tarzını kapsar ve risk yönetim felsefesi ve risk iştahı, dürüstlük ve etik değerler ile faaliyet gösterilen ortamı kapsayacak şekilde işletme çalışanlarının riski nasıl gördüğü ve riske karşı nasıl hareket edeceklerine ilişkin bir temel oluşturur (Steinberg, 2011, s. 82).

İç çevre KRY'nin diğer unsurları için disiplin ve yapı sağlayan bir temel oluşturur. Stratejilerin ve amaçların nasıl geliştirileceğini, işletme faaliyetlerinin nasıl yapılandırılacağını ve risklerin nasıl belirleneceğini ve değerlendirileceğini etkiler.

Ayrıca kontrol faaliyetlerinin, bilgi ve iletişim sistemlerinin ve izleme faaliyetlerinin nasıl tasarlanacağını etkiler (Reding vd., 2013, s. 4-6).

İç çevre işletmenin kültüründen etkilenir. COSO'nun da üzerinde durduğu aşağıdaki unsurlardan oluşur (Reding vd., 2013, s. 4-6).

- İşletmenin yürüttüğü her faaliyette riski nasıl dikkate aldığını karakterize eden paylaşılan inançlar ve tavırlar setini yansıtan risk yönetimi felsefesi.
- İşletme çapında bir bakış açısıyla, işletmenin kabul etmeye istekli olduğu risk miktarını yansıtan risk iştahı.
- İşletmenin gözetiminde birincil yönetim organı olarak rol oynayan, işletmeye deneyim ve bağımsızlık sağlayan yönetim kurulu.
- İşletmenin tercihleri, davranış standartları ve tarzını yansıtan dürüstlük ve etik değerler.
- Bir göreve atanmak için gerekli olan bilgi ve beceriyi ifade eden yetkinliğe bağlılık.
- Planlama, icra, kontrol ve izleme faaliyetleri için bir çerçeveyi oluşturan örgütsel yapı.
- Problemlerin çözülmesi için görevlendirilen ve desteklenen bireylerin veya ekiplerin belirlenmesini ya da tersine yetki sınırlamalarını ifade eden yetki ve sorumlulukların atanması.
- İşe alım, oryantasyon, eğitim, değerlendirme, danışma, destekleme ve düzeltici önlemlerden oluşan insan kaynakları standartları.

#### *3.4.2.3.2. Amaç belirleme*

KRY çerçevesinde iç çevreden hemen sonra gelen amaç belirleme unsuru, yönetime etkili bir KRY süreci oluşturmasında destek sağlamak amacıyla önemli koşulları düzenlemektedir. Bu unsur, etkili bir iç çevreye ek olarak, işletmenin misyonuyla uyumlu ve operasyonel, raporlama ve uygunluk faaliyetlerini kapsayan bir dizi stratejik amaç belirlemesi gerektiğini dikte eder. COSO KRY, bir misyon ifadesinin amaç belirlemenin önemli bir unsuru olduğunu vurgular; misyon amaca yönelik genel bir ifadedir ve belirli fonksiyonel stratejilerin geliştirilmesi için bir yapı taşıdır. Basit, açık bir misyon ifadesi, bir işletmenin amaçlarını ve risklere yönelik tutumunu özetlemelidir. Düzgün bir şekilde geliştirilmiş bir misyon ifadesi, işletmenin yüksek seviyede stratejik amaçlar geliştirmesini ve daha sonra operasyonel, uygunluk ve raporlama amaçları seçmesini ve

uygulamasını desteklemelidir. COSO KRY işletmelerin misyon ifadesiyle doğrudan bağlantılı amaçları geliştirmelerini ve risk yönetimi amaçlarına ulaşılıp ulaşılmadığını değerlendirmek için ölçütler geliştirmelerini istemektedir (Moeller, 2009, s. 130).

Amaçlar; faaliyet, uygunluk ve raporlama amaçlarına bir temel oluşturacak şekilde stratejik bir düzeyde belirlenir. Bütün işletmeler çeşitli iç ve dış kaynaklı risklerle karşılaşırlar ve etkin bir olay tanımlama, risk değerlendirme ve riske yanıt verme süreci için amaçların geliştirilmesi bir önkoşuldur. Amaçlar, işletmenin risk tolerans düzeyini yönlendiren risk iştahıyla uyumlu olarak düzenlenmelidir. Risk toleransı amaçlara ulaşılmasıyla ilişkili olarak kabul edilebilir seviyedeki büyüklük ve çeşitlilikte olmalıdır ve işletmenin risk iştahıyla uyumlu olarak düzenlenmelidir.

Risk iştahı bir işletmenin almayı kabullendiği risk oranıdır ve işletmenin risk yönetim felsefesini yansıtır. Risk toleransı ise, işletme amaçlarına ulaşılması konusunda kabul edilebilir fark seviyesidir. İşletme faaliyetlerinin risk toleransını dikkate alarak yürütülmesi, işletmenin risk iştahı sınırı içerisinde kalarak amaçlarına ulaşmasını sağlar (PWC, 2006, s. 20).

KRY'nin iç çevre unsurunun iki temel çıktısı vardır. Bunlardan ilki, işletmenin risk yönetimi felsefesinin tanımlanması ve anlaşılması; ikincisi ise, işletmenin risk iştahının onaylanmasıdır. Bu iki çıktı, amaç belirleme bileşeninin risklerle uyumlu birçok amaç geliştirmesine ve risk toleransı açısından risk iştahının belirlenmesine izin verir. Toleranslar bir işletmenin her seviyedeki riskleri kabul edip etmeyeceğini değerlendirirken kullanması gereken rehberler ve ölçülerdir. Birçok işletme için risk toleranslarının oluşturulması ve uygulanması çok zor olabilir. Eğer kurallar açıkça tanımlanmaz, iyi anlaşılmaz ve katı bir şekilde uygulanmazsa problemler yaşanacaktır (Moeller, 2011, s. 65).

#### *3.4.2.3.3. Olay tanımlama (Risk tanımlama)*

Olay tanımlama, yönetimin işletmenin stratejisini uygulama ve amaçlarına ulaşma becerisini etkileyen riskli olayları doğru bir şekilde algılama kabiliyetini ifade eder. Yöneticiler ve çalışanlar için olası olumsuz etkileri olan olayları belirlemek kesinlikle önemli olmakla birlikte olumlu durumları da belirlemeleri zorunludur. Potansiyel olumsuz etkileri olan olayların işletmenin KRY sürecinde kontrol altına alınması gerekirken; potansiyel olumlu etkilere sahip olanların işletmenin misyonu, vizyonu ve risk iştahı açısından gözden geçirilmesi gerekir (Cendrowski ve Mair, 2009, s. 93).

Olayların tanımlanmasında, uygulayıcıların rekabet ortamındaki faktörleri, makroekonomik etkenleri ve çalışan sorunlarını yalnızca zaman içindeki statik bir noktada değil, aynı zamanda bu değişkenlerdeki eğilimleri belirleme amacı ile de gözlemlemeleri gerekir. Böyle yapmak, işletme gelecekteki olayları tahmin etmek için trend çizgilerini kullanabileceği için riskler hakkında daha iyi planlama olanağı sağlayabilir. Ayrıca işletmenin olaylar meydana geldiğinde, işletme üzerindeki etkilerini tartışan merkezi bir veri tabanına sahip olması önemlidir. Böylece yöneticilerin daha çabuk geçmişten ders çıkarmalarına ve bu dersleri yeni çalışanlar ve risk yöneticileri ile paylaşmalarına olanak tanınmış olur.

Yönetim olayları tanımlarken, işletmenin risk kapsamı bağlamında risk ve fırsatlar doğurabilecek çeşitli iç ve dış faktörleri değerlendirir. Dış faktörler şunlardır (Reding vd., 2013, s. 4-7):

- Ekonomik Olaylar: Fiyat hareketleri, sermaye kullanılabilirliği ve pazara girişte zayıf engeller gibi olaylardır.
- Doğal Çevre Olayları: Sel, yangın, deprem gibi olaylardır.
- Politik Olaylar: Yeni yasa ve düzenlemelerin yanı sıra seçim sonuçları işletmeler üzerinde önemli etkilere neden olabilir.
- Sosyal Faktörler: Deprem gibi bir doğa olayı aniden meydana gelirken, sosyal faktörler yavaş yavaş gelişen olaylardır. Bunlara demografik değişiklikler, sosyal harcamalar, toplumsal ihtiyaçlar, aile yapıları ve bir işletmeyi ve müşterilerini zaman içinde etkileyebilecek diğer olaylar dâhildir.
- Teknolojik Olaylar: Örneğin yeni elektronik ticaret, depolama veya işleme araçlarının ortaya çıkması gibi olaylardır.

İç faktörler ise şunlardır (Reding vd., 2013, s. 4-7; Moeller, 2009, 132):

- Altyapı Faktörleri: Sermaye tahsisinin artırılmasından, önleyici bakımlara ve çağrı merkezi desteğine kadar riskle ilişkili temel faktörlerdir.
- Çalışanlarla İlgili Faktörler: İş kazaları, hileli faaliyetler, iş sözleşmesinin sona ermesi gibi olaylardır.
- Süreçle İlgili Faktörler: Süreç değişiklikleri, süreç yürütme hataları ve dış kaynak kullanımı kararları gibi faktörlerdir.
- Teknolojik Faktörler: Her işletme, resmi risk tanımlama ihtiyacını tetikleyebilecek çok çeşitli teknolojik olaylarla karşı karşıyadır. Güvenlik ihlalleri ve sistem kesintileri gibi olaylardır.

Bir işletme önemli risk taşıyan olayları net bir şekilde tanımlamalı ve daha sonra bunları izlemek için gerekli tüm önlemleri alabilecek süreçlere sahip olmalıdır. Bu geleceğe dönük süreci birçok işletmede belirlemek zordur. İç ve dış potansiyel risk taşıyan olaylara bakarak hangilerinin daha fazla dikkat gerektirdiğine karar vermek zor bir süreç olabilir. Bazıları acil ihtiyaçlar gerektirirken, birçoğu geleceğe yönelik olabilir. COSO KRY, olay tanımlama konusunda kullanıcılara destek sağlamaktadır. COSO rehberi işletmelerin aşağıdaki yaklaşımları kullanmalarını tavsiye etmektedir (Moeller, 2009, s. 133):

- Olay Envanteri: Yönetim, işletmeye özel endüstri kolunda ve fonksiyonel alanda riskle ilgili yaygın olay listelerini geliştirmelidir. Başka bir deyişle, işletme, öğrenilen dersler türünden bir arşiv kaynağı kurmayı düşünmelidir. Bu arşiv, işletmenin daha uzun çalışma süresine sahip çalışanları tarafından sağlanan ve daha önceki tecrübeleri içerisinde barındıran verilerden oluşur.
- Çalıştay: Bir işletme, çeşitli iç veya dış olaylardan kaynaklanabilecek olası risk faktörlerini tartışmak için fonksiyonlar arası çalıştaylar geliştirebilir. Bu çalıştayların sonucunda potansiyel riskleri düzeltmek için yapılacak eylem planları elde edilecektir. Yaklaşım iyi görünse de, genellikle risk hakkında tartışmak için yeterli zaman ayırmak zor bir iştir.
- Görüşmeler ve Anketler: Potansiyel risk olaylarıyla ilgili bilgi, müşteri memnuniyeti mektupları veya çalışanlarla yapılan görüşmeler gibi çok çeşitli kaynaklardan gelebilir. Bu bilgi, bir risk olayına işaret edebilecek herhangi bir durumu tanımlamak için ele alınmalı ve sınıflandırılmalıdır.
- Süreç Akış Analizi: COSO KRY uygulama teknikleri, süreçleri gözden geçirmek ve olası riskli olayları belirlemek için akış diyagramlarının kullanılmasını önerir. Bu akış şemaları iç kontrol için kullanılanlara benzer.
- Başlıca Olay Göstergeleri: İşletmeler olaylarla ilişkili verileri izleyerek bir olaya neden olabilecek koşulların varlığını belirler. Örneğin, finansal kuruluşlar, geç ödemelerle nihai kredi temerrüdü arasındaki ilişkiyi ve erken müdahalenin olumlu etkisini uzun zamandır fark etmiştir. Ödeme modellerinin izlenmesi, temerrüde düşme olasılığının zamanında önlem alınmasıyla azaltılmasına olanak tanır.
- Kayıp Olay Verisinin İzini Sürme: Gösterge tablosu yaklaşımı riskli olayları ortaya çıktığında izlerken, biraz zaman geçtikten sonra elde edilen veriler olayları belli bir perspektiften görmek açısından değerlidir. Kayıp olayların izini sürmek, ilgilenilen

alanlardaki faaliyetlerin izini sürmek için hem dâhili hem de kamu veri tabanlarının kullanılmasını yansıtır. Bu kaynaklar, başlıca ekonomik göstergelerden dahili ekipman arıza oranlarına kadar geniş bir yelpazeyi kapsayabilir. Bir işletme, riskle ilişkili hem iç hem de dış olayların izini sürmek için etkin risk tanımlama süreçleri geliştirmelidir.

#### *3.4.2.3.4. Risk değerlendirme*

Risk değerlendirme bir işletmenin potansiyel olayların amaçların başarılmasını nasıl etkileyebileceğini göz önüne alma becerisini tanımlar. Bu riskler nitel ve nicel yöntemlerin bir kombinasyonu kullanılarak olasılık ve etki olmak üzere iki boyutta değerlendirilir. Herhangi bir olay türüne göre çok sayıda potansiyel sonuç bulunmaktadır. Yöneticiler, bu sonuçları uygun bir risk karşılığı geliştirmede değerlendirmelidir.

Uygulayıcılar, riskleri iki boyutta değerlendirmelidir, doğal ve artık riskler. Doğal riskler, bir etkinliğin kendisinin doğasına özgü risklerdir. Örneğin, bir kuruluşun bütçesinde hataların olması riski, bütçenin büyüklüğüyle birlikte artar. Artık riskler ise, bir risk yönetimi planı tanımlandıktan ve belirli riskler azaltılmaya çalışıldıktan sonra bile kalan risklerdir. Bu riskler, herhangi bir işletmede daima mevcuttur (Cendrowski ve Mair, 2009, s. 94).

Bu iki kavram, işletmenin her zaman bazı risklerle karşı karşıya kalacağını gösterir. Yönetim, risk tanımlama süreciyle ortaya çıkardığı riskleri ele aldıktan sonra bile, düzeltilmesi gereken bazı artık riskler olacaktır. Ayrıca bazı doğal riskler yönetim tarafından az da olsa azaltılabilir. Örneğin bir işletme pazar hâkimiyetiyle ilgili bazı doğal riskleri azaltmak için adımlar atabilirken büyük bir depremle ilgili doğal risklere hiçbir şey yapamayacaktır.

Olasılık ve etki, risk değerlendirmesi yapmak için gerekli olan diğer iki temel bileşendir. Olasılık, bir riskin meydana gelme ihtimalidir. Birçok durumda riskin meydana gelme olasılığını yüksek, orta ve düşük şeklinde ifade eden temel bir yönetim değerlendirmesi gereklidir. Olasılık tahminleri geliştirmek için bazı iyi nicel araçlar da vardır ancak güçlü destekleyici veriler olmaksızın riskin ortaya çıkma ihtimalini tahmin etmek çok iyi sonuçlar vermeyecektir (Moeller, 2009, s. 134).

Riskli bir olayın etkisini tahmin etmek daha kolaydır. Örneğin BT ile ilişkili riskler için, bir veri sunucusunun ya da ağ merkezinin çökmesinin etkisi; işletmenin tesis ve donanımın değiştirilmesinin maliyeti, sistemleri tekrar yükleme maliyeti ve BT'lerinde

yaşanan ilgili arıza nedeniyle yapılamayan işlerin maliyeti gibi nispeten daha doğru tahminler geliştirilebilir. Bununla birlikte KRY, bu risklerle ilgili kesin, aktüeryal düzeydeki hesaplamaları geliştirmek değil, etkili bir risk yönetimi çerçevesi oluşturmaktır. Ayrıntılı hesaplamalar sigortacıların görevidir.

Bir dizi nicel ve nitel ölçümle, risk olasılığı ve potansiyel etkilerin bir analizi geliştirilebilir. COSO KRY uygulama tekniklerinden risk olasılığı ve etkilerinin belirlenmesinde veri kaynağı olarak faydalanılabilir. Temel amaç belirlenen tüm riskleri değerlendirmek ve bunları tutarlı bir şekilde olasılık ve etki açısından sıralamaktır. Ayrıntılı bir nicel analiz yapılmadan tanımlanan her bir risk, etkisi ve olasılığı değerlendirilerek 1 ila 10 arasında bir göreli ölçekte sıralanabilir. Bu sıralama tanımlanan her bir riski inceleyen ve daha sonra bu ölçeğe göre sıralayan bir yönetim karar süreciyle başarıya ulaşabilir. Daha büyük işletmelerde riskler 1-10 arasında ölçeklendirilmek yerine 1-100 arasında daha ayrıntılı olarak ölçeklendirilebilir. Bu uygulamanın temel amacı yönetimin odaklanması gereken riskleri belirlemektir (Moeller, 2009, s. 136). Tablo 3.1 örnek bir risk değerlendirme analizinin küçük bir bölümünü göstermektedir.

**Tablo 3.1.** *Risk Değerlendirme Analizi (Moeller, 2008, s. 260)*

| Risk Adı | Risk Tanımı | Etki | Olasılık | Risk Puanı |
|---|---|---|---|---|
| Muhasebe Riski | Satış faaliyetinin doğru ve zamanında kaydedilmemesi, finansal raporların yanlış olduğunu gösterebilir. | Yüksek: Muhasebe hatalarının finansal ve operasyonel bilgi üzerinde önemli bir etkisi olabilir | Orta: Güçlü yordamlara rağmen, işletme içinde çeşitli konumdaki yeni personel hatalar yapabilir. | 8 |
| Yasal Risk | Yürürlükteki veya sürekli değişen yasaları ve düzenlemeleri anlamamak, birçok faaliyetin uygunsuzluğuna yol açabilir. | Orta: Birçok düzenlemenin küçük, teknik ihlallerinin bile faaliyetler üzerinde önemli bir etkisi olmamalıdır. | Yüksek: Birden fazla düzenlemenin etkisindeki uluslararası faaliyetlerde ihlaller ortaya çıkabilir. | 7 |
| Görevlerin Ayrılması | Görevlerin ayrılığı kontrollerinde yetersizlik, çalışanların yetkisiz süreçlerde yer almasına ve hileli işlemleri yapmasına izin verir. | Yüksek: Hileli işlemler işletme faaliyetleri üzerinde önemli etkilere neden olabilir. | Düşük: Devam eden iç denetimler ve daha güçlü yönetim-kontrol uygulamaları bu tür kontrol problemlerini önleyecektir. | 5 |

#### *3.4.2.3.5. Risk tepkisi*

Riskleri değerlendiren yönetim, nasıl tepki vereceğini belirler. Risk tepkisi; kaçınma, azaltma, paylaşma ve kabul etme seçeneklerini kapsar. Yönetim, risk tepkisini değerlendirirken, istenen risk tolerans seviyesi içerisinde kalan bir artık risk düzeyi sağlayan tepkiyi seçerek risk olasılığı ve etkisinin yanı sıra maliyetler ve faydalar üzerindeki etkisini değerlendirir. Yönetim, mümkün olabilecek bütün fırsatları belirler ve genel artık riskin işletmenin risk iştahı içerisinde olup olmadığını belirleyen işletme çapında risk görünümünü ele alır (Reding vd., 2013, s. 4-8). Risk tepkisi seçenekleri aşağıda açıklanmıştır (Moeller, 2009, s. 136):

- Kaçınma: Riski yüksek bir iş birimini satmak, riskli bir üretim hattını terk etmek veya riskli bir coğrafi alanda bulunan faaliyetlerine son vermek gibi bir riskten uzaklaşma stratejisinin uygulanmasıdır. İşletmenin riskli bir üretim hattından ayrılmasının çoğu zaman mümkün olmaması veya riskli olayla ilişkili maliyetler ortaya çıktıktan sonra uzaklaşılamaması stratejinin zorlayıcı tarafıdır. Bir işletme çok düşük seviyede bir risk iştahına sahip olmadıkça, gelecekte ortaya çıkabilecek potansiyel bir risk yüzünden başarılı bir iş alanından ya da ürün grubundan uzaklaşması mümkün değildir. Risk almaktan kaçınmak için riskli alanlardan çıktıktan sonra başka alanlara çoğu zaman daha fazla yatırım yapılmak zorunda kalınması, kaçınmayı potansiyel olarak masraflı bir strateji yapar.
- Azaltma: Bazı iş kararlarıyla belirli riskler azaltılabilir. Ürün çeşitlendirmesi yapmak tek bir ürün grubuna güvenmenin sebep olduğu risklerin önüne geçebilir veya BT faaliyetlerini iki coğrafi alana bölmek kötü sonuçlar doğurabilecek arıza risklerini engelleyebilir.
- Paylaşma: Birçok işletme düzenli olarak risklerinin bir kısmını sigorta alımı yoluyla paylaşır ancak diğer risk paylaşım teknikleri de mevcuttur. Bir işletme muhtemel fiyat dalgalanmalarından korunmak amacıyla finansal riskten korunma işlemleri (vadeli işlem, opsiyon gibi.) yapabilir veya potansiyel iş risklerini ortak girişim (joint venture) anlaşmaları ya da diğer yapısal düzenlemeler yoluyla paylaşabilir. Ana fikir, başka bir tarafın potansiyel bir riski veya bir kısmını kabul etmesi ve bunun sonucunda risklerle beraber ortaya çıkan tüm kazançları da paylaşmasıdır.
- Kabul Etme: Potansiyel bir riski azaltmak için hiçbir girişimde bulunmaksızın bir işletmenin kendi kendini güvence altına aldığı durumlar gibi bir eylemsizlik stratejisidir. Temelde bir işletme belirlenen risk toleransı ışığında risk olasılığını ve

etkisini değerlendirmeli ve ardından bu riski kabul edip etmeyeceğine karar vermelidir. Risk olasılığı ve etkisini değiştirmek için hiçbir eylemde bulunmamaktır. Kabul etme bir şirketin karşılaştığı çeşitli risklerin çoğu için uygun bir strateji olabilir.

Yönetim, riskten kaçınma stratejilerinin birinin veya bir karışımının etrafında inşa edilmiş bir yaklaşımı kullanarak risklerinin her biri için genel bir tepki stratejisi geliştirmelidir. Bunu yaparken her bir potansiyel risk tepkisinin faydalarını ve maliyetlerini karşılaştırmalı ve şirketin genel risk iştahına en iyi uyan stratejileri seçmeye çalışmalıdır. Birçok risk için uygun tepkiler açıktır ve hemen hemen herkes tarafından anlaşılır. Örneğin bir BT işlemi, temel veri dosyalarını yedeklemek için zaman ve kaynakları harcıyor ve bir iş sürekliliği planı uyguluyor. Böyle temel yaklaşımların gerekliliği konusunda genellikle hiç kuşku yoktur, ancak çeşitli yönetim kademeleri yedekleme süreçlerinin sıklığını veya süreklilik planının ne sıklıkta sınanması gerektiğini sorgulayabilir. Yani, planlanan risk tedbirlerinin kapsamını ve maliyetini sorgulayabilirler.

#### *3.4.2.3.6. Kontrol faaliyetleri*

KRY'nin kontrol faaliyetleri, belirlenen risk tepkisine göre harekete geçmek için gerekli olan politika ve yordamlardan oluşur. Bu faaliyetlerin bazıları yalnızca bir işletme alanında tanımlanmış ve onaylanmış bir risk tepkisi ile ilgili olarak geliştirilse de genellikle birden fazla fonksiyon veya birim üzerinde yürütülmektedir. COSO KRY'nin kontrol faaliyetleri bileşeni, riske tepki verme stratejileri ve eylemleriyle sıkı bir şekilde ilişkilendirilmelidir. Bir işletme uygun risk tepkilerini seçtikten sonra risk tepkilerinin zamanında ve etkili bir şekilde yürütülmesini sağlamak için gerekli kontrol faaliyetlerini seçmelidir. Yaygın olarak kullanılan kontrol faaliyetlerine aşağıdakiler örnek verilebilir (Moeller, 2009, 139):

- Üst Düzey İncelemeler: Üst düzey yöneticiler, organizasyon birimleri içerisinde tanımlanan risk olaylarının farkında olmalı ve belirlenmiş risklerin durumu hakkında düzenli olarak üst düzey değerlendirmeler yapmalıdır.
- Fonksiyonel İncelemeler: Üst düzey incelemelere ek olarak, fonksiyonel ve direkt birim yöneticileri, risk-kontrol faaliyetlerinin izlemesinde önemli bir role sahip olmalıdır. Bu rol, özellikle kontrol faaliyetleri, kurumsal kanallar arasında iletişim

ve risk çözümlemesi ihtiyacı olan ayrı işletme birimleri içerisinde yürütüldüğünde daha fazla önem kazanır.

- Bilgi İşleme: İster BT ekipmanları ister kayıtla yürütülsün, bilgi işleme bir işletmenin riskle ilişkili kontrol faaliyetleri için önemli bir bileşendir. İşletmenin BT süreçleri ve riskleri üzerinde durularak uygun kontrol yordamları oluşturulmalıdır.
- Fiziksel Kontroller: Riskle ilgili birçok endişe stoklar, menkul kıymetler, demirbaşlar gibi fiziksel varlıklar içindir. Bir işletme fiziksel envanterler, teftişler veya güvenlik yordamları gibi riske dayalı fiziksel kontrol faaliyetlerini uygulamalıdır.
- Performans Göstergeleri: Günümüzde genellikle her işletme, risk olayıyla ilgili performans raporlamasını da destekleyen çok çeşitli finansal ve operasyonel raporlama araçlarını kullanmaktadır. Gerekli olduğu durumlarda, bu önemli KRY kontrol faaliyeti bileşenini desteklemek amacıyla performans araçları ihtiyaca göre düzeltilmeli ya da değiştirilmelidir.
- Görevlerin Ayrılığı: Klasik bir kontrol faaliyeti olarak, belirli eylemleri başlatan kişi, asla onları onaylayan kişi olamaz.

#### *3.4.2.3.7. Bilgi ve iletişim*

Bilgi, işletme içi ve dışındaki kaynaklardan toplanmalı, belgelendirilmeli ve bir işletmenin tüm paydaşlarına zamanında iletilmelidir. İlgili bilgi, kişilerin sorumluluklarını yerine getirmelerini sağlayan şekilde ve zamanında belirlenmeli, toplanmalı ve iletilmelidir. Ayrıca bilgi, işletmeden müşteriler, tedarikçiler ve düzenleyici kurumlar gibi tüm ilgili taraflara akmalıdır.

Bilgi, bir işletmenin riski tanımlama, değerlendirme ve tepki verme ihtiyaçları ile yeterli tutarlılıkta olmalıdır. Bilgi sistemleri, dahili ve harici olarak üretilen verileri, riskleri yönetmek için yararlı olan bilgilere dönüştürür. Son olarak bilgi, karar almayı desteklemek için yeterli kalitede olmalıdır. COSO bilginin sahip olması gereken genel özellikleri şöyle sıralamıştır (Reding, 2013, s. 4-9):

- Uygun ve doğru detay seviyesinde olmalıdır.
- Zamanında ve ihtiyaç duyulduğunda kullanılabilmelidir.
- En son finansal ve operasyonel bilgileri yansıtacak şekilde güncel olmalıdır.

- Doğru ve güvenilir olmalıdır.
- Birisi ihtiyaç duyduğunda erişebilmelidir.

Birçok işletme, çok sayıda BT aracına ve iletişim yöntemine sahiptir. Bazen bu araçlardan gelen çok fazla miktarda bilgi, kullanıcıları zorlayabilir. Bir yönetici bir günde çok sayıda e-posta almaktadır. Bir zamanlar elektronik bir mucize olarak görülen şeyler, şimdi birçokları için bir sıkıntı haline gelmiştir. Bilginin iletilmesinde yöneticilerin bu sorunu kavramaları önem taşır. Çalışanlara çok kısa bir süre içinde çok fazla bilgi aktarılırsa, bu bilgi bütünüyle anlaşılmayabilir veya ihmal edilebilir. Araştırmalar, bir organizasyonda güçlü iletişim araçlarının varlığının yeterli ve uygun iletişimi sağlamak için yeterli olmadığını göstermiştir. Bunun yerine esnek bir kültür, stratejik planlama, BT entegrasyonu ve tedarikçi ilişkileri gibi maddi olmayan tamamlayıcı işletme ve insan kaynaklarını etkili bir şekilde kullanan işletmeler iyi iletişimin faydalarını elde edeceklerdir (Cendrowski ve Mair, 2009, s. 95-96).

Etkili iletişim aşağı, yukarı ve yatay bilgi akışını sağlar. Tüm çalışanlar üst yöneticilerden KRY sorumluluklarını üstlenmeleri hakkında açık bir mesaj alırlar. Kurumsal risk yönetiminde kendi sorumluluklarını ve kendi faaliyetlerinin başkalarının işleriyle nasıl ilişkili olduğunu anlarlar. Önemli bilgi akışını sağlayan etkili iletişime sahip olmalıdırlar. Ayrıca müşteriler, tedarikçiler, düzenleyici kurumlar ve hissedarlar gibi dış paydaşlarla da etkili bir iletişim kurulmalıdır (Reding, 2013, s. 4-10).

#### *3.4.2.3.8. İzleme*

İzleme faaliyetlere eşlik etmek, test etmek, incelemek ve uygun kişilere raporlamak anlamına gelir. İzleme faaliyetinin amacı planlanan tedbirlerin ve süreçlerin uygulamaya geçirilip geçirilmediğinin doğrulanması, söz konusu tedbirlerin ve risklere karşı geliştirilen tepkilerin riskleri risk iştahı içerisinde tutup tutmadığının belirlenmesi ve izlemeler sonucunda tespit edilen problemlere karşı gerekli faaliyetlerin yürütülmesinden oluşur (Morris, 2005, s. 254).

KRY çerçevesinin temeline yerleştirilen izleme, KRY unsurlarının etkili bir şekilde çalışıp çalışmadığını belirlemek için gereklidir. İşletmedeki çalışanlar, destek süreçleri, iç ve dış koşullar değişirken izleme unsuru, KRY'nin sürekli olarak etkin bir şekilde çalışmasına yardımcı olur. İzleme, diğer KRY unsurlarının faaliyetlerinde bulunan sapmaları ve ihlalleri yakalar. Örneğin, müşteri faturaları zamanında ödenmezse, alacak hesaplarını faturalayan birim, genel finansal ve operasyonel riskleri tanımlayabilmelidir.

Kredi tahsilatlarını izleyen araçlar, tahsilatların durumuna ilişkin veriyi günü gününe üst yönetime sağlamalıdır (Moeller, 2008, s. 269).

KRY unsurlarının zaman içinde varlığı ve işleyişini değerlendirmek amacıyla izlenmesi gerekir. Böyle bir yukarıdan aşağıya kontrol, ancak devam eden izleme faaliyetleri, ayrı değerlendirmeler veya bu ikisinin bir kombinasyonu yoluyla sağlanabilir. Devam eden izleme, genellikle günlük yönetim faaliyetlerinin normal seyrinde gerçekleşir. Ayrı değerlendirmelerin doğası, kapsamı ve sıklığı, öncelikle yönetimin risk değerlendirmelerine ve mevcut devam eden izleme yordamlarının etkinliğine bağlıdır. İzleme faaliyetleri sonucunda saptanan eksiklikler, yukarı yönlü raporlanmalı ve önemli hususlar üst yönetim ve yönetim kuruluna iletilmelidir (Reding, 2013, s. 4-10).

İzleme faaliyeti, işletmede uygun kontrollerin uygulandığına, KRY süreçlerinin doğru konumlandırıldığına ve faaliyetlerin riske tepki vermek amacıyla geliştirilen stratejilerle uyumlu olduğuna dair güvence sağlar. Bu sürece yön veren ve çalışmalara temel oluşturan belgeler; yönetim performans sonuçları, yönetim kurulu ve risk komitesi raporları, denetim komitesi toplantı tutanakları ve raporları, kontrol raporları, risk değerlemeleri eylem planı ve iç denetim raporu olarak sıralanabilir (Pehlivanlı, 2010, s. 88).

İzlemeler sonucunda risklerin tam ve doğru olarak ölçümünde sorunlar olduğu, risk sınıflandırmalarında yanlışlıklar yapıldığı ve raporların asıl sorumluların eline ulaşmadığı gibi sorunlar varsa bunlar ortaya çıkarılır ve böylelikle gerekli tedbirlerin alınması sağlanabilir (Benson, 2007, s. 85). İzleme süreci, gerekli tedbirlerin alınıp alınmadığını da inceler.

### *3.4.2.4. Kurumsal risk yönetiminin faydaları*

KRY'nin yararlarının işletmeye göre değişeceği unutulmamalıdır. Bununla birlikte, kurumsal risk yönetimi uygulamaları genel olarak bir organizasyonun performans ve karlılık hedeflerine ulaşmasına ve kaynak israfını önlemesine katkı sağlar. IIA, KRY'nin faydalarını şöyle sıralamıştır (IIA, 2004, s. 3):

- "Amaçlara ulaşılması olasılığının arttırılması;
- Çeşitli risklerin yönetim kurulu seviyesinde konsolide raporlanması;
- Temel riskler ve etkilerinin daha iyi anlaşılması;
- İşletme risklerinin belirlenmesi ve paylaşılması;
- Yönetimin daha önemli konulara odaklanabilmesi;
- Daha az sürpriz ve krizin yaşanması;
- Doğru işlerin doğru yöntemlerle yapılmasına daha fazla odaklanılması;
- Değişim girişimlerinin başarıya ulaşılma olasılığının artırılması;
- Daha fazla kazanç elde edebilmek için daha fazla risk alabilme yeteneği;
- Bilgiye daha fazla dayanan risk belirleme ve karar alma süreçleri."

Her işletme karşılaştığı zorlukları belirleyebilmeye ve bu zorlukları gidermek için risklere uyum sağlamaya ihtiyaç duyar. İşletmeler, hem değer yaratma fırsatlarının hem de değere ulaşılmasını zorlaştıran risklerin farkında olarak karar alma süreçlerini yürütebilmelidir. Kısacası kurumsal risk yönetimi uygulamalarını strateji belirleme ve performans yönetimi ile bütünleştirmelidir. Böylece işletme, risk yönetimi sürecinden birçok fayda elde edebilecektir. COSO çerçevesi temel olarak bu faydaları aşağıdaki başlıklar altında özetlemiştir (COSO, 2016, s. 6):

- Fırsatların Arttırılması: Bütün makul olasılıkları göz önünde bulundurarak yönetim, işletme için fırsatları ve mevcut fırsatlarla ilişkili benzersiz zorlukları tanımlayabilir. Örneğin, bir gıda işletmesinin yöneticileri, işletmenin sürdürülebilir gelir artışı amacını etkileyebilecek potansiyel riskleri göz önünde bulundurduklarında, işletmenin birincil müşterilerinin giderek sağlık bilinciyle hareket ettiklerini ve alışkanlıklarını bu doğrultuda değiştirdiklerini belirleyebilirler. Bu değişim, bir belirsizliği gösterir: işletmenin mevcut ürünlerine olan talepte gelecekte potansiyel bir azalma tehdidi söz konusudur. Buna karşılık yönetim, yeni ürünler geliştirme ve mevcut ürünleri iyileştirme yollarını devreye sokarak, işletmenin mevcut müşterilerinden elde ettiği gelirin korunmasını (değeri koruma) ve daha geniş bir tüketici tabanına hitap ederek ek gelir yaratılmasını (değer yaratma) sağlayabilir.

- İşletme Çapında Risklerin Belirlenmesi ve Yönetilmesi: Her işletme, işletmenin birçok parçasını etkileyebilecek sayısız riskle karşı karşıya kalır. Bazen bir risk, işletmenin bir bölümünden kaynaklanabilir ancak farklı bir bölümünü de etkiler. Yönetim, performansı sürdürmek ve geliştirmek için işletme çapında riskleri tanımlamalı ve yönetmelidir. Örneğin, bir banka ticari faaliyetlerinde çeşitli risklere maruz kaldığının farkına vardığında yönetim, dahili işlemleri ve ilişkili harici bilgi tarafından desteklenen piyasa bilgisini analiz etmek için bir sistem geliştirerek cevap vermelidir. Böyle bir sistem birimler, müşteriler ve çalışanlar için detaylı inceleme imkânı sağlayan tüm ticari faaliyetlerin içindeki risklerin kapsamlı bir görünümünü sağlar. Aynı zamanda bankanın riskleri ölçmesine izin verir. Böyle bir sistem işletmenin KRY gerekliliklerini karşılar ve bankanın risklere daha etkin yanıt vermek için daha önce birbirinden kopuk durumda olan verilerini bir araya getirmesine izin verir.
- Sürprizlerin ve Kayıpların Azaltılması: Kurumsal risk yönetimi organizasyonların potansiyel riskleri belirleme ve uygun cevaplar geliştirme, sürprizleri ve ilişkili maliyetleri veya kayıpları azaltma becerilerini geliştirmelerini sağlar. Örneğin, müşterilerine üretimlerinde kullanmaları için tam zamanında parça sağlayan bir üretim işletmesi, parçaları zamanında teslim edemediği için cezalar ödeme riskiyle karşılaşabilir. Bu riske karşılık olarak işletme teslimat günleri, teslimat rotaları ve teslimat filosundaki planlanmamış onarımlar gibi faktörleri gözden geçirerek nakliye süreçlerini değerlendirebilir. Elde ettiği bulguları teslimat filosu için bakım çizelgeleri ayarlamak, teslimatları sıkışık dönemler dışında planlamak ve önemli güzergâhlara alternatifler bulmak için kullanabilir. Tüm gecikmelerin engellenemeyeceğini kabul ederek, müşterileri potansiyel gecikmeler konusunda uyarmak için yordamlar geliştirebilir. Böylece yönetim, yetenekleri dâhilinde riski etkileyerek (üretim ve planlama) ve direkt etkisinin ötesinde risklere uyum sağlayarak (gecikmeler) performansı geliştirmiş olur.
- Performans Değişkenliğinin Azaltılması: Bazı işletmelerde performans değişkenliği konusundaki zorluklar; sürprizler ve kayıplar konusundakilere göre daha fazladır. Ayrıca planlanandan daha kısa zamanda ya da beklentilerin üzerinde performans göstermek en az beklentilerin altında kalmak kadar endişe uyandırır. Örneğin, bir toplu taşıma sistemini kullananlar için 10 dakika erken hareket etmek en az 10 dakika gecikme kadar sinir bozucu olacaktır, çünkü ikisinde de kullanıcılar

zarar görme riskiyle karşılaşacaklardır. Bu değişkenliği yönetmek için, planlayıcılar programa doğal duraklar koyacaklardır. Sürücüler tasarlanan duraklarda programa uymak için belirli bir zamana kadar bekleyeceklerdir. Bunu yapmak seyahat sürelerinde değişkenliklerin düzelmesine yardımcı olur, taşıma sisteminin genel performansını geliştirir ve kullanıcıların görüşlerini iyileştirir. KRY, işletmelerin performansı etkileyecek riskleri öngörmesine ve bozulmayı en aza indirgemek için harekete geçmelerine izin verir.

- Kaynak Dağıtımının Geliştirilmesi: Risk konusunda sağlam bilgi edinmek yönetimin genel kaynak ihtiyaçlarını değerlendirmesine ve kaynak tahsisini artırmasına olanak tanır. Örneğin, bir gaz dağıtım şirketi, yaşlanan altyapısının bir gaz kaçağı riskini arttırdığını belirleyebilir. Gaz sızıntısı ile ilgili verilere ilişkin eğilimleri inceleyen kuruluş, dağıtım ağındaki riskleri değerlendirmeyi başarmalıdır. Yönetim daha sonra yıpranmış altyapıyı yenileme ve faydalı ömürleri kalan bölümleri onarmaya yönelik bir plan geliştirebilir. Bu yaklaşım, işletmenin altyapı bütünlüğünü sürdürmesine ve önemli ek kaynakların daha uzun bir zaman periyodunda tahsis edilmesine izin verir.

KRY, işletme yönetiminin riske ilişkin tutarlı kararlar alabilmesi için uygun metotlar ve teknikler sağlar. Böylece üst yönetimin karar alma süreçlerindeki belirsizliğini azaltır. İşletmede reaktif yönetim tarzından daha proaktif yönetim tarzına geçilmesini destekler. Ayrıca KRY, işletmenin amaçlarına ulaşabilmesi için gerekli olan risk yönetiminin sağlamlığına ilişkin makul seviyede güvence sağlar (Pehlivanlı, 2010, s. 69).

KRY'nin iç denetçiler açısından en önemli faydalarından biri, iç denetçinin risk algısını değiştirerek, işletmenin amaçlarına ulaşmasının önündeki risklere odaklanmasını sağlamasıdır. Böylece iç denetçinin işletmeye değer katma işlevi ön plana çıkar (Walker vd., 2003, s. 54). Diğer taraftan KRY süreçlerinden beklenen faydanın elde edilebilmesi sistemin etkin çalışıp çalışmadığına bağlıdır. Eğer iç denetim birimi KRY'de güvence rolü üstlenmişse, KRY'nin etkinliğinin değerlendirilmesi, alınması gereken önlemlerin önerilmesi ve sürecin takibinde önemli rol oynar (Pehlivanlı, 2010, s. 70).

### *3.4.2.5. Yeni Kurumsal Risk Yönetimi Çerçeveleri*

Son yıllarda kurumsal risk yönetimi anlayışında yaşanan dönüşüm, iki önemli risk yönetimi çerçevesinin güncellenmesini gerektirmiştir. COSO, ilk defa 2004 yılında yayımladığı kurumsal risk yönetimi çerçevesini, işletme dünyasının değişen koşullarını ve ortaya çıkan yeni gereksinimleri dikkate alarak güncellemiştir. 2016 yılında yeni kurumsal yönetim çerçevesinin taslağını yayınlamış, 2017 yılında paydaşlarının geri bildirimleriyle desteklediği çerçevesini Kurumsal Risk Yönetimi - Strateji ve Performansla Riskin Düzenlenmesi adıyla yürürlüğe koymuştur. COSO çerçevesinden sonra dünyada yaygın olarak kullanılan ikinci risk yönetimi çerçevesi, Uluslararası Standardizasyon Örgütü (ISO- The International Organization for Standardization) tarafından ilk defa 2009 yılında yayımlanan çerçevedir. ISO çerçevesini, işletmelerin karşılaştıkları yeni zorlukları ve değişimleri dikkate alarak, 2018 yılında ISO31000:2018 Risk Yönetimi Rehberi adıyla yeniden yayımlamıştır.

#### *3.4.2.5.1. Yeni COSO KRY Çerçevesi (COSO KRY 2)*

Yeni COSO KRY çerçevesi, üst yöneticiler, yönetim kurulları, risk çalışanları ve iç denetçilerden oluşan uygulayıcıların kabul düzeyini artırmak, adaptasyonlarını sağlamak ve KRY faaliyetlerinin bütünleştirilmesini kolaylaştırmak amacıyla iş süreçleri bakış açısıyla hazırlanmıştır. Bir organizasyonun, genellikle operasyonel yönetiminden ayrı yürütülen, iş süreçlerinden kopuk risk yönetimi faaliyetlerinin bütünleştirilmesi gerektiğini savunur. Yeni kurumsal risk yönetimi anlayışıyla, işletmede risk yönetiminin iş süreçlerinden bağımsız kişiler tarafından yürütülen ve aşamalı olarak ilerleyen bir faaliyet olarak algılanmasının önüne geçilmek istenmiştir. Çünkü çalışanların, süreçlerin ve teknolojilerin arasında bütünleşme eksikliği faaliyetleri zorlaştırır ve KRY'nin işletme faaliyetlerine ilişkin öngörüler elde ederek ve tavsiyeler sunarak sağlayabileceği değerin yaratılmasını engeller. Yeni COSO KRY çerçevesi, daha önce 8 unsurdan oluşturduğu ve küp şeklinde betimlediği risk yönetimi modelini, birbiriyle ilişkili 5 unsurdan oluşan bir sarmalla ifade etmiştir (Prinsenberg & Sluis, 2017, s. 14; COSO, 2016, s. 6). Şekil 3.6 yeni çerçevenin unsurlarını gösterir.


**Şekil 3.6.** *COSO KRY Sarmalı (COSO, 2016)*

1. Yönetişim ve kültür: Yönetişim, organizasyonun risklerini tanımlayan, kurumsal risk yönetimi yapısını güçlendiren ve gözetim sorumluluklarını geliştiren kurumun yönetim tarzını düzenler. Kültür; etik değerler, istenen davranışlar ve kurumdaki risk anlayışı ile ilgilidir.

2. Strateji geliştirme ve amaçların belirlenmesi: Kurumsal risk yönetimi, stratejik planlama süreçlerinde strateji ve amaç belirleme faaliyetleriyle birlikte çalışır. Risk iştahı belirlenir ve strateji ile uyumlu hale getirilir. İşletme amaçları; riskin belirlenmesi, değerlendirilmesi ve uygun tepkilerin geliştirilmesi için bir temel oluştururken, stratejilerle uygulamaya konur.

3. Performans: Strateji ve işletme amaçlarına ulaşılmasını etkileyebilecek risklerin belirlenmesi ve değerlendirilmesi gerekir. Stratejiler ve amaçlara ulaşılması performansla ilişkilidir. Riskler, risk iştahı üzerindeki ağırlıklarına göre önceliklendirilir. Organizasyon daha sonra risk tepkilerini seçer ve üstlendiği risk miktarına ilişkin bir risk portföyü oluşturur. Bu sürecin sonuçları anahtar risk paydaşlarına bildirilmektedir.

4. İncele ve revize et: Bir kurum, işletme performansını gözden geçirerek, kurumsal risk yönetimi unsurlarının zaman içinde önemli değişikliklere bağlı olarak ne kadar iyi çalıştığını ve hangi revizyonların gerekli olduğunu incelemeli ve gerektiğinde revize etmelidir.

5. Bilgi, iletişim ve raporlama: Kurumsal risk yönetimi, işletme içi ve dışı kaynaklardan gerekli bilgilerin elde edilmesi ve gerektiğinde paylaşılmasını sağlayan iletişim kanallarını oluşturmalıdır. Bu kanallar hem işletme içinde yukardan aşağıya ve aşağıdan yukarıya hem de işletme dışında iletişim kurulması gereken bilgi kaynakları ve paydaşlarla sürekli olarak iletişimi sağlamalıdır.

Güncellenen çerçevedeki beş bileşen, bir dizi ilke tarafından desteklenir. Bu ilkeler, yönetişimden izlemeye kadar her şeyi kapsar. İşletmenin türü veya faaliyet gösterdiği sektörden bağımsız olarak, işletmenin büyüklüğüne göre farklı şekillerde uygulanabilecek ilkelerdir. Bu ilkelere bağlı kalınması, üst yönetim ve yönetim kuruluna, işletmede stratejiyi ve amaçları etkileyen risklerin anlaşılması ve yönetilmesi konusunda makul bir beklenti sağlayabilir. Yeni çerçeve 20 ilkeden oluşur. İlkeler, Şekil 3.7'de gösterilmiştir.


**Şekil 3.7.** *COSO KRY İlkeleri (COSO, 2016)*

Çerçeve, "jargon" riskini ortadan kaldırmaya çalışmakta, kavramları ve uygulamaları tartışmak için ortak işletme dilini benimsemektedir. Çerçeve, aynı dilin kullanılmasıyla KRY'nin kurum tarafından kabul görmesinin ve benimsenmesinin teşvik edileceğini savunmaktadır. Geleneksel uygulamada KRY, bir işletme birimini, ekibi ya da savunma hatlarının bir parçasını ifade etmesine karşın, yeni çerçevenin getirdiği bütüncül bakış açısı, bir işletmede riskin yönetilmesi için kullanılan kültürün, yeteneklerin ve faaliyetlerin risk kapsamında tartışılmasını sağlar. Yeni çerçevenin KRY'ye getirdiği temel değişiklikler, Tablo 3.2'de yer almaktadır (Prinsenberg & Sluis, 2017, s. 12):

**Tablo 3.2.** *COSO KRY 2'nin Getirdikleri (COSO, 2016)*

| |
|---|
| **Yeni bir çerçeve yapısı**: İş yaşam döngüsüne uygun 5 risk bileşeni ve 20 ilke, işletme içinde risk iletişiminin daha güçlü olmasını sağlamıştır.<br>**Risk yönetimini bütünleştirmeye odaklanma**: Riskin strateji belirleme ve günlük işletme faaliyetleriyle ilişkilendirilmesi, KRY ilkelerinin değer yaratmayı ve değerin korunmasını desteklemek için kullanılmasına yardımcı olur.<br>**KRY çerçevesinin iş süreçleri perspektifiyle hazırlanması**: Yeni KRY çerçevesinde riskle ilgili kavramlar, bir organizasyonun KRY'den gerçek faydalar elde etmesine olanak veren değerin yaratılması açısından tartışılmıştır.<br>**İşletmenin her yönetim kademesinde risk yönetiminin açıklanması:** İşletmenin tamamından bir işletme birimindeki yordamları etkileyen risklere kadar uzanan bir bakış açısı, KRY'yi yalnızca işletmenin çevresindeki risklerden izole etmeyi amaçlamaktan çok daha fazlasına dönüştürür.<br>**Kültüre daha fazla vurgu**: Günümüz piyasalarının değişen talep ve beklentilerini yansıtan bir KRY modeli, organizasyonun sorumlu olduğu tüm risklerin yönetilmesini sağlar.<br>**KRY'nin farklı faydalarının araştırılması**: Zararların azaltılmasından stratejik danışmanlığa kadar eksiksiz bir çerçevenin tasarımı hakkında bilgi sunar.<br>**Risk ve performans arasındaki ilişkiyi vurgulayan grafikler**: Risk seviyesi ile performans arasındaki ilişkiyi tanımlayıp değerlendirmenin yeni bir yolunu gösterir.<br>**Zorlu konular hakkında daha derin tartışmalar**: Risk iştahı ve risk görünümü gibi konuların daha kolay tartışılmasını sağlar.<br>**Teknolojinin gelişen rolünün incelenmesi**: Teknolojinin bir organizasyonun stratejisini, iş süreçlerini ve risk yönetimini nasıl etkileyebileceğinin tartışılmasına imkân tanır.<br>**Örnekler üzerinde incelemeler sunması**: İlkelerin çeşitli sektörlerde ve işletme türlerinde nasıl uygulanacağını vurgular. |

Strateji belirleme süreci, kurumsal risk yönetiminin bütünleşmesi gereken önemli bir faaliyet alanıdır. Stratejik hatalar, operasyonel başarısızlıklara kıyasla hisse değerindeki kayıpların büyük çoğunluğunun temel sebebidir. Araştırmalar, organizasyonların strateji geliştirme süreçleriyle kurumsal risk yönetimi arasındaki ilişkiyi keşfettiklerini ve iki faaliyet arasında bütünleşmeyi sağlamak istediklerini göstermektedir. Şekil 3.8 misyon, vizyon ve çekirdek değerlerin şekillendirdiği stratejilerin işletmenin genel yönetiminin ve performansının itici gücü olduğunu göstermektedir. İşletme faaliyetleri ve süreçleriyle bütünleşen KRY, daha iyi karar almayı ve performans artışını sağlayan çok daha tutarlı bilgi mimarisinin geliştirilmesini sağlar. KRY, işletmenin değer zinciri döngüsünün tamamında risk bilgisiyle hareket edilmesini sağlamalıdır.


**Şekil 3.8.** *COSO KRY'de Strateji, İşletme Amaçları ve Performans (COSO, 2016)*

KRY işletmenin strateji geliştirme, performans yönetimi, amaç belirleme ve yönetişim süreçleriyle bütünleştirilmelidir. Bütüncül bakış açısıyla KRY, işletmenin çeşitli seviyelerinde risk yönetimi faaliyetlerinin yürütülmesini ve risk bilgisiyle hareket edilmesini sağlayabilir (Richtermeyer, 2018, s. 25). KRY'yi iş süreçleriyle bütünleştirmek, karar alma süreçlerini destekleyen daha iyi bilgi ve iletişim yapısının ve daha yüksek performansa ulaşılmasının önündeki engelleri ortadan kaldırır. KRY, risk bilinciyle karar vermeyi tesis eder. Risk bilinciyle performansı etkileyen kararlar optimize edilir. Risk bilinciyle alınan kararların işletmenin risk profilini nasıl etkilediği tespit edilir. Şekil 3.9 KRY'nin bütünleştiği iş süreçlerine sunduğu risk bilinciyle karar verme yapısını gösterir (Sobel, 2018, s. 16). KRY'yi iş süreçleriyle bütünleştirmek, aşağıdaki faydaları sunar:

- Risklerin ortaya çıkmadan önce açık şekilde öngörülmesini sağlar.
- Mevcut ve yeni fırsatlar belirlenir ve takip edilir.
- Performanstaki sapmalara daha hızlı ve tutarlı bir şekilde cevap verilir.
- Kapsamlı ve tutarlı bir bütüncül risk görünümü geliştirir ve her örgütsel seviyeye raporlanmasını sağlar.
- İşbirliği, güven ve bilgi paylaşımını iyileştirir.


**Şekil 3.9.** *Risk Bilinciyle Karar Verme (Sobel, 2018, s. 16)*

İşletmelerin KRY'den amaçlanan faydaları elde etmeleri için, organizasyonun KRY faaliyetleriyle elde edebileceği faydalar önceden tespit edilmeli, güçlü bir KRY yapısı oluşturmak için organizasyon içinde istenen bütünleşmenin kapsamı belirlenmeli, mevcut kültür, yetenekler ve faaliyetleri geliştirmek için gerekli girişimlerin başlatılması ve kaynakların doğru yerlere harcanmasını sağlayan önceliklendirmenin yapılması gerekir. KRY faaliyetlerinin ve çerçevesinin geliştirilmesi için gereken öncelikli adımlar Tablo 3.3'te sunulmuştur:

**Tablo 3.3.** *KRY'nin Geliştirilmesi İçin Gereken Adımlar (COSO, 2016)*

| |
|---|
| KRY çerçevesini uygulamak ve geliştirmek için yönetim kurulu, ilgili YK komiteleri ve üst yönetimin onayı alınmalıdır. |
| Karar alma süreçlerinin risk yönetimiyle bütünleştirilmesi teşvik edilmeli ve gereken eğitimler verilmelidir. |
| Risk yönetimi rolleri ve sorumlulukları netleştirilmeli ve gerekli iletişim sağlanmalıdır. |
| Risk yönetimi faaliyetlerini ve karar vermeyi destekleyen araçlara ve teknolojiye yatırım yapılmalıdır. |
| BT sağlayıcıları, tedarikçiler ve ilgili üçüncü taraflar, risk ve performans tartışmalarına dâhil edilmelidir. |
| Karar alma süreçlerinin bir parçası olarak, işletmenin risk iştahı ve profili yönetişim organlarında tartışılmalıdır. |
| Mevcut faaliyetlerin, organizasyonun KRY beklentileriyle ve istenen bütünleşmeyle uyumlu olup olmadığı değerlendirilmelidir. |
| Geliştirme fırsatlarının ortaya çıkarılması amacıyla risk belirleme, değerlendirme, önceliklendirme ve müdahale süreçleri gözden geçirilmelidir. |
| Performans raporlaması ile daha fazla bütünleşme fırsatlarını sunan raporlama uygulamaları analiz edilmelidir. |

Yeni COSO Çerçevesi, kurumsal risk yönetiminin teknolojik gelişmeleri takip etmesinin önemli olduğunu vurgulamaktadır. KRY faaliyetlerinin ve yeteneklerinin, işletme dünyasındaki değişimlerin, ortaya çıkan ve değişen risklerin hızına uyum sağlaması gerekmektedir. Bilgi, İletişim ve Raporlama ilkeleri, bütünleşik risk ve performans raporlamasının işletmeler için bir zorunluluk haline geldiğini gösterir. Güçlü KRY'nin geliştirilmesi amacıyla işletmeler, Büyük Veri ve Yapay Zekâ teknolojileri gibi yeni nesil veri analitiklerini ve teknolojilerini kullanmalıdır. Teknoloji altyapısı, KRY'de verinin doğruluğu, tamlığı ve zamanlılığını sağlayacaktır (Herron & Dholabhai, 2017, s. 21).

Hiç şüphe yok ki işletmeler; değişiklikler, karmaşıklıklar ve belirsizliklerle dolu bir gelecekle yüzleşmeye devam edecektir. KRY, bir işletmenin böyle dönemlerde nasıl yönetileceğinin ve yönlendirileceğinin önemli bir parçası olacaktır. Bir işletmenin türüne ve büyüklüğüne bakılmaksızın, stratejilerinin misyonuna bağlı kalması gerekir. Tüm organizasyonların, güçlü karar verme süreçleriyle paydaşlarına karşı yüksek güven düzeyini korurken, kapasitesinin çok çabuk uyarlanabilmesi dahil değişime tutarlı bir şekilde cevap verebilen özelliklere sahip olmaları gerekmektedir. KRY'nin, öngörülen faydalarını tutarlı bir şekilde sağlamak için geleceğe adapte olması gerekecektir. KRY doğru konulara odaklanarak, işletmelere geleceği öngörebilme kabiliyetleri konusunda güven sağlayabilir. Geleceğe baktığımızda, KRY üzerinde etkili olacak birkaç eğilimin olduğu göze çarpar (COSO, 2016, s.7-8):

**Veri hacminin çoğalmasıyla uğraşma**: KRY'nin giderek daha fazla verinin daha hızlı analiz edilebildiği yeni veri analitiği teknolojilerine uyum sağlaması gerekmektedir. İşletmenin hem içinden hem de dışından daha fazla veri toplanabilecek, yeni yöntemlerle işlenebilecektir. Gelişmiş veri analitiği ve görselleştirme araçları, risklerin hem olumlu hem de olumsuz etkilerinin daha iyi anlaşılmasını geliştirecek ve KRY faaliyetlerine çok faydalı olacaktır.

**Yapay zekâ ve otomasyondan yararlanma:** Günümüzde birçok insan, otomatik süreçler ve yapay zekâ dönemine girdiğimizi düşünmektedir. KRY faaliyetlerinde ve uygulamalarında otomasyon, yapay zekâ ve gelecekte keşfedilecek teknolojilerin etkisinin göz önünde bulundurulması ve KRY yeteneklerinin arttırılması önemlidir. İleri teknoloji araçlarıyla önceden tanınmayan ilişkiler, eğilimler ve modeller ortaya çıkarılabilir ve bu da risk yönetimi için kritik bir bilgi kaynağı sağlar.

**Risk yönetimi maliyetini yönetme**: Birçok işletme yöneticisi tarafından çok sık dile getirilen bir endişe, kazanılan değere kıyasla risk yönetiminin, uygunluk faaliyetlerinin ve kontrol süreçlerinin maliyetidir. Kurumsal risk yönetimi uygulamaları geliştikçe, risk yönetimi, uygunluk, kontrol ve yönetişimi kapsayan faaliyetlerin organizasyona maksimum fayda sağlamak için etkin bir şekilde koordine edilmesi ve güçlü işbirliğiyle yürütülmesi önem kazanacaktır. Bu durum, KRY'nin organizasyon için önemini yeniden tanımlaması için en iyi fırsatlardan birini temsil edebilir. KRY, risk yönetimi, uygunluk, kontrol ve yönetişim faaliyetlerinin daha düşük maliyetle, koordinasyon ve işbirliğiyle yürütülmesini sağlayan yapının merkezinde yer alabilir.

**Daha güçlü organizasyonlar inşa etme**: İşletmeler, KRY'yi strateji ve performansla bütünleştirmede daha iyi hale geldikçe, esnekliği güçlendirme fırsatı kendini gösterecektir. İşletmeler, faaliyetleri üzerinde büyük etkiye sahip olacak risklerin farkında olarak, daha çabuk hareket etmelerine olanak sağlayan yeteneklerini geliştirmek için KRY'yi kullanabilirler. Böylece, KRY yeni fırsatların değerlendirilmesine destek olacaktır.

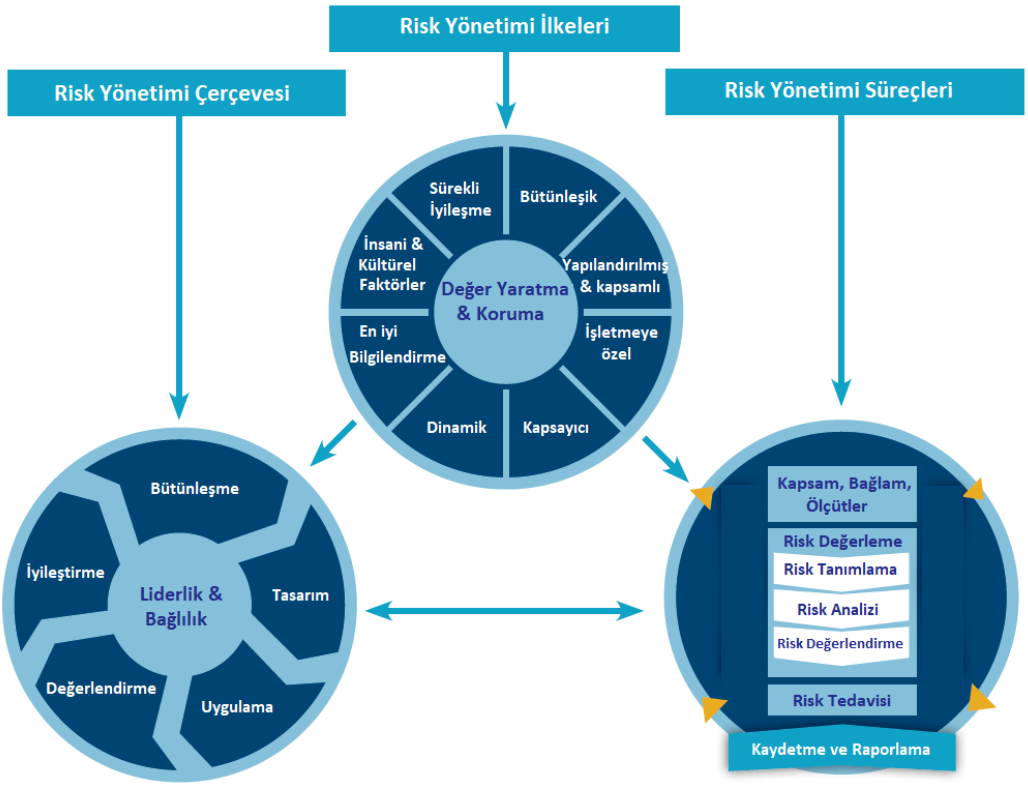
#### *3.4.2.5.2. Yeni ISO 31000 Risk Yönetimi Rehberi*

ISO, ilk defa 2009 yılında yayımladığı risk yönetimi çerçevesini, Şubat 2018'de yeni COSO KRY çerçevesiyle aynı değişiklikleri vurgulayan şekliyle ve benzer bakış açısıyla güncellemiştir. Bununla birlikte, ISO 31000 Risk Yönetimi Rehberinin risk yönetiminin stratejik ve operasyonel bir yönetim sistemiyle bütünleştirilmesi olan genel amacı aynı kalmıştır. 2018 sürümünün ana değişiklikleri aşağıda tanımlanmıştır (IRM, 2018, s. 8):

- Üst yönetim tarafından liderliğin önemi, organizasyonun yönetişimi ve risk yönetiminin bütünleşmesi vurgulanmıştır.
- Risk yönetiminin sürekli tekrar eden yapısına daha fazla önem atfedilmiştir. Yeni bilgi ve analizler sürekli olarak süreçlerin, eylemlerin ve kontrollerin revize edilmesini sağlamalıdır.
- KRY'nin kapsamı, ihtiyaçlara çok hızlı cevap verebilen sistemlerden oluşan modelinin sürdürülmesine daha fazla odaklanacak şekilde düzenlenmiştir.

ISO 31000'in yeni sürümü önceki sürümden daha kısadır ve risk yönetiminin nasıl uygulanabileceğine ilişkin bütüncül bir bakış sunmaktadır. ISO 31000, etkin risk

yönetimini niteleyen ilkeler, çerçeve ve süreçleri önermektedir. ISO 31000'in 2018 sürümü tarafından benimsenen genel yapı ve yaklaşım, Şekil 3.10'da gösterilmektedir. Şekil incelendiğinde, yeni ISO rehberinin, yeni COSO çerçevesiyle aynı risk yönetimi anlayışına sahip olduğu, risk bilgisiyle desteklenen karar alma süreçlerine daha fazla önem atfettiği, değer yaratılması ve korunmasını ilkelerinin merkezine yerleştirdiği ve etkili risk yönetimi için örgütsel ve teknolojik bütünleşmeyi savunduğu anlaşılır (IRM, 2018, s. 9).

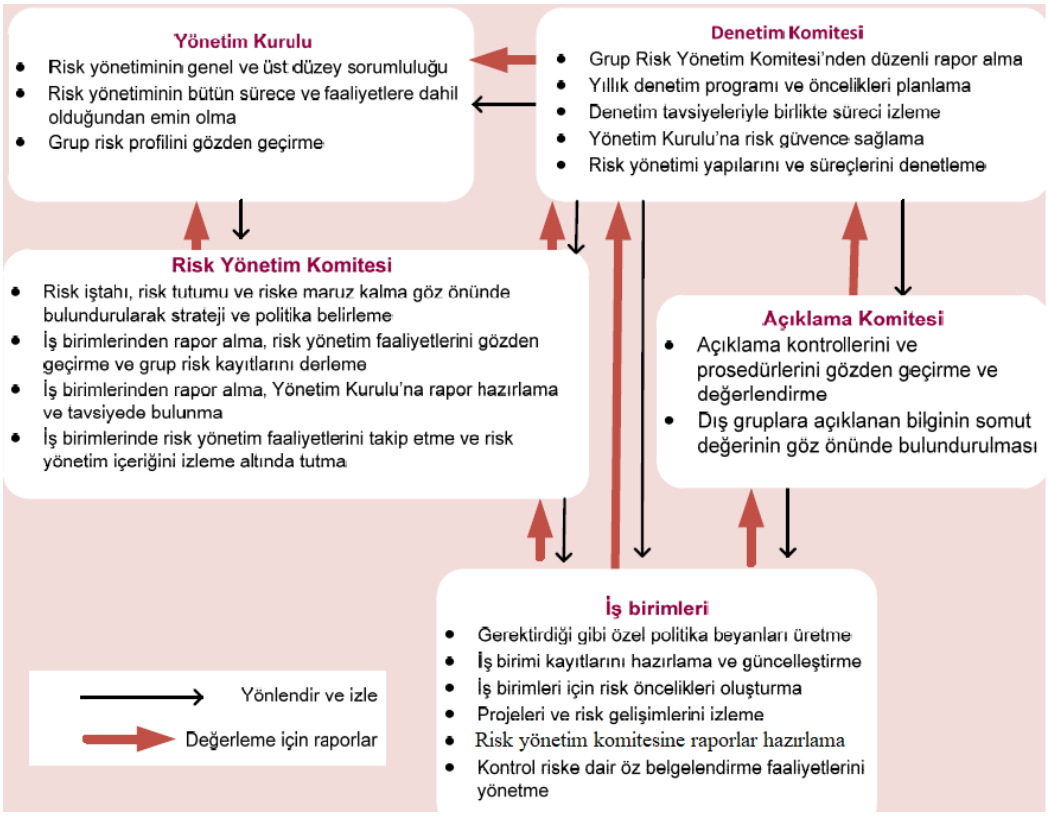



**Şekil 3.10.** *ISO31000*

ISO 31000 rehberi, KRY ilkelerinin; risk yönetimi, karar alma, amaç belirleme ve amaçlara ulaşılması doğrultusunda çaba gösterme ve performans yükseltme faaliyetleriyle organizasyonlarda değer yaratmak ve değerin korunmasından sorumlu tüm çalışanlar tarafından uygulanması gerektiğini belirtir. İlkeler, her tür ve büyüklükte işletmede uygulanabilir ve tüm iç ve dış faktörler ve etkiler ile ilgilidir. Ayrıca, ilkeler KRY'nin kuruluşlara strateji belirleme, amaçlara ulaşma ve bilgilendirilmiş karar alma süreçleri konusunda destek olması gerektiğini belirtmektedir. Risk yönetimi, yönetişimin ve liderliğin bir parçasıdır ve kuruluşların her örgütsel seviyesinin nasıl yönetildiğinin temelini oluşturur. Yeni ISO31000 rehberinin sekiz ilkesi şunlardır (IRM, 2018, s. 10):

1. KRY çerçevesi ve süreçleri işletmeye uygun şekilde özelleştirilmelidir.
2. Uygun paydaşların zamanında katılımı gereklidir.
3. Yapısal ve kapsamlı bir yaklaşım gereklidir.
4. Risk yönetimi, tüm organizasyonel faaliyetlerin ayrılmaz bir parçası olmalıdır.
5. Risk yönetimi değişiklikleri öngörür, tespit eder, tanır ve cevap verir.
6. Risk yönetimi mevcut bilginin yol açtığı herhangi bir sınırlamayı açıkça dikkate almaktadır.
7. İnsani ve kültürel faktörler risk yönetiminin tüm yönlerini etkiler.
8. Risk yönetimi, öğrenme ve deneyim yoluyla sürekli geliştirilir.

KRY'nin başarısı için, işletme ölçeğinde planlı bir çaba gerekir. Ancak risk yönetimi standartlarının uygulanması aniden mümkün olmayan aşamalı bir süreçtir. İşletme yönetimi tarafından risk yönetimi politikaları geliştirilmelidir. Risk yönetimi politikalarında, işletmenin iç kontrol ve risk yönetimi amaçlarına, riske karşı eylem tarzlarına, risk farkındalığı kültürünün ve denetim ortamının geliştirilmesi çabalarına ve risk iştahı olarak tanımlanan kabul edilebilir risk seviyesine yer verilmelidir. Ayrıca risk yönetimi politikaları; risk analizi ve raporlama için gereken belgelendirmeyi, risk tanımlama faaliyetlerinin ayrıntılarını, organizasyon ve yordamlar için gereken düzenlemeleri ve risk tepkisi olarak tanımlanan risk azaltma ve kontrol mekanizmalarını düzenler. Risk yönetimi sorumlulukları, eğitim konuları ve öncelikleri, izleme ve karşılaştırma ölçütleri ve uygun kaynakların tahsisi risk politikalarının kapsaması gereken diğer önemli konulardır. Kısacası, politikalar işletmenin risk mimarisini açıklamalıdır. Şekil 3.11, ISO31000 Çerçevesine göre, büyük ölçekli bir işletmenin risk mimarisinin özetini sunar (IRM, 2010, s.11).




**Şekil 3.11.** *ISO31000 Risk Mimarisi (IRM, 2010)*

### *3.4.2.6. Kurumsal risk yönetimi (KRY) mi? Yönetişim-risk-uygunluk (YRU) mu?*

Geniş kapsamlı bir kavram olan yönetişim, risk yönetimi ve uygunluk (YRU), kurumsal risk yönetimi (KRY), operasyonel risk yönetimi, sorun yönetimi ve diğer ilişkili kavramları bünyesinde barındırır (Ramanathan, 2010, s.1). Sadece risk yönetimi sorunlarını çözmeye yönelik olarak hazırlanan çerçeveler genellikle kurumsal risk yönetimi (KRY) olarak adlandırılır. Kurumsal risk yönetiminin bünyesinde bulunması gerektiği varsayılan özellikler, yönetişim-risk yönetimi-uygunluk (YRU) çerçevelerinin de içerisinde de yer alır. Bu çerçeveler risk yönetimine ek olarak hem yönetişimi hem de uygunluğu kapsar (Dupuis vd., 2011, s. 319).

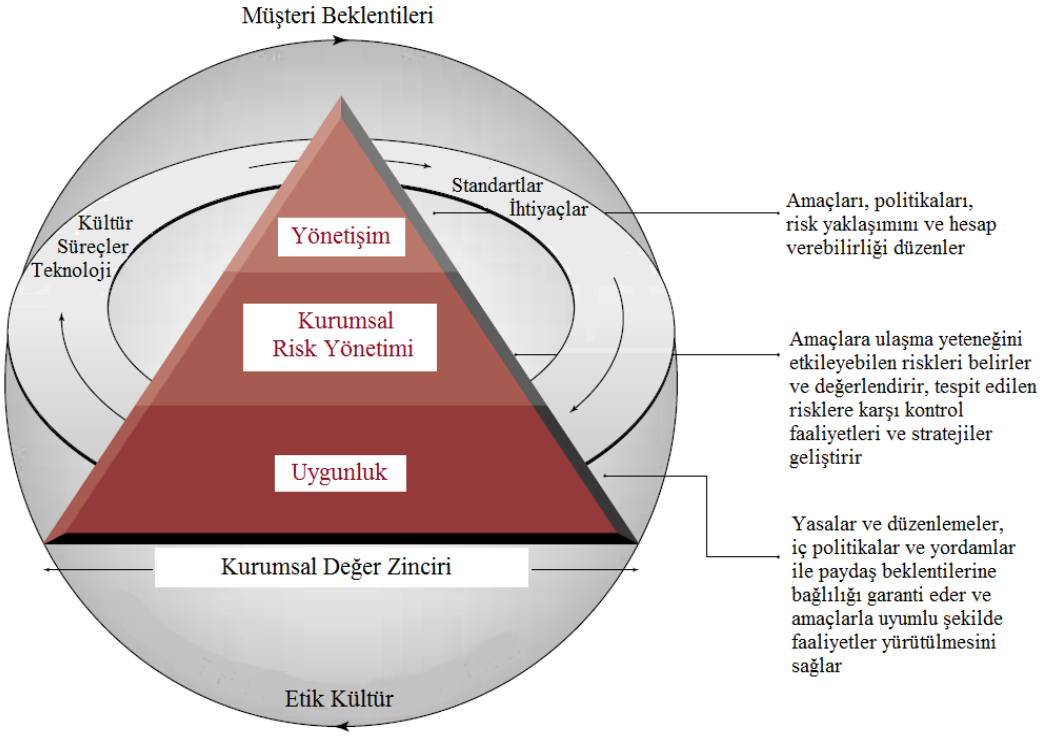
On yıl kadar önce KRY, sadece risk değerlendirme olarak görülmekteydi, YRU ise daha fazla uygunluk ve iç kontrol odaklıydı. Değişen koşullar ve ihtiyaçlar neticesinde, günümüzde KRY hala risk odaklı olmasının yanı sıra YRU'nun kapsamına giren kontroller, testler ve izlemeyi de kapsamaktadır. YRU ise uygunluk ve yönetişim süreçlerinin yanında giderek daha fazla risk odaklı bir yaklaşımı benimsemiştir. Sonuç olarak günümüzde standart bir YRU tanımı dikkate alındığında, KRY'nin onun bir alt kümesi haline geldiği görülür. YRU, KRY'den farklı olarak daha fazla şeffaflık ve hesap

verebilirliği vurgular, daha fazla uygunluk ve belirlenen ölçütlere bağlı olma meyillidir ve kontrol yapısına daha fazla odaklanmıştır (Mont, 2016, s. 36)

YRU kavramı ortaya çıkmadan önce, risk yönetimi konusunda işletme çapında bir bakış açısıyla KRY bir çerçeve olarak mevcut bulunmaktaydı. İç denetçiler, KRY'nin değerini kavramak ve YRU ile nasıl bütünleştirileceğini değerlendirmek zorundadır. Hangisinin diğerinden üstün olduğunu düşünmek veya mesleki bir bakış açısıyla hangisinin doğru veya yanlı olduğunu düşünmek anlamsızdır. Ne YRU riske ilişkin bol miktarda ve güvenilir veri olmadan ne de KRY riski yönetişim, uygunluk, strateji ve iş performansıyla bütünleştirmeden doğru çalışabilir (Adams, 2016, s. 16).

Hem YRU hem de KRY bir işletmenin karşı karşıya kaldığı bütün riskleri tanımlamayı, analiz etmeyi ve sayısal olarak miktarını ifade etmeyi amaçlar. Fakat önemli bir farklılık vardır. KRY bütün risk çeşitlerini yönetmek için, riskin sayısal olarak ölçülmesine ve işletmenin risk yaklaşımının geliştirilmesine yönelik bir metodoloji sağlar. YRU, raporlama mekanizmaları için teknolojiden faydalanarak yönetişim ve uygunluk riskleri etrafında risk ve kontrol fonksiyonlarının iletişimini ve işbirliğini sağlayan daha geniş ve kapsayıcı bir çerçeve ve felsefedir. YRU politikalar, yordamlar, belgeleme gereksinimleri ve risk değerlendirmeleri gibi konuları organize eder ve merkezileştirir. Kısacası YRU, KRY'ni kapsar (Banham, 2007, s. 49).

YRU'nun alt kümelerinden biri olan kurumsal risk yönetimi (KRY) (Jefferson Wells, 2009, s. 1) yasalara ve düzenlemelere uygunluğu da kapsayan risk faktörlerinin dikkate alınmasını ve etkili raporlamayı amaçlar. Kurumun itibarının zarar görmesinden ve bununla ilişkili sonuçlardan kaçınmaya destek olur. Gelecekte belirsizlik yaratabilme potansiyeline sahip olayları belirler, kontrol altında tutar ve izler. İşletmenin amaçlarına ulaşmasını etkileyen fırsatlar ve tehditlerin belirlenmesi, tanımlanması, değerlendirilmesi, bunlara karşı işletmenin alacağı pozisyonun kararlaştırılması ve rapor edilmesi için işletme çapında uygulanan yapılandırılmış, tutarlı ve sürekli devam eden bir süreçtir (IIA, 2004, s. 3). Kurumsal Risk Yönetimi, YRU süreçlerinin merkezinde yer alır (Bkz. Şekil 3.12).




**Şekil 3.12.** *YRU Süreçleri İçinde Kurumsal Risk Yönetimi (PWC, 2004, s. 7)*

YRU ile kurumsal risk yönetimi (KRY) arasındaki ilişki bir tartışma konusudur. Ortaya atılan bir görüşe göre YRU, KRY artı yönetişim ve uygunluğun toplamı olarak tanımlanır, diğer taraftan diğer görüş KRY'nin yönetişim riskini ve uygunluk riskini zaten yönettiğidir (Mitchell, 2008, s. 72). Aslında YRU'nun temel bileşenleri tek başlarına ele alındıklarında da, diğer bileşenleri göz önünde bulundurur. Örneğin, yönetişim, uygunluğu ve risk yönetimini kapsar veya uygunluk uzmanları yönetişim ve riski uygunluk faaliyetleri olarak nitelendirmektedir. Bu bakış açılarının ortak noktası, YRU faaliyetlerinin birbirleriyle uyumlu bir şekilde çalıştığı ve önemli ilişki içerisinde olduklarıdır. YRU; bilgi akışını, etkileşimli süreçleri ve kapasiteyi bütünleştiren çalışanlar, süreçler ve teknolojinin bir araya getirilmesidir (Mitchell, 2008, s. 73).

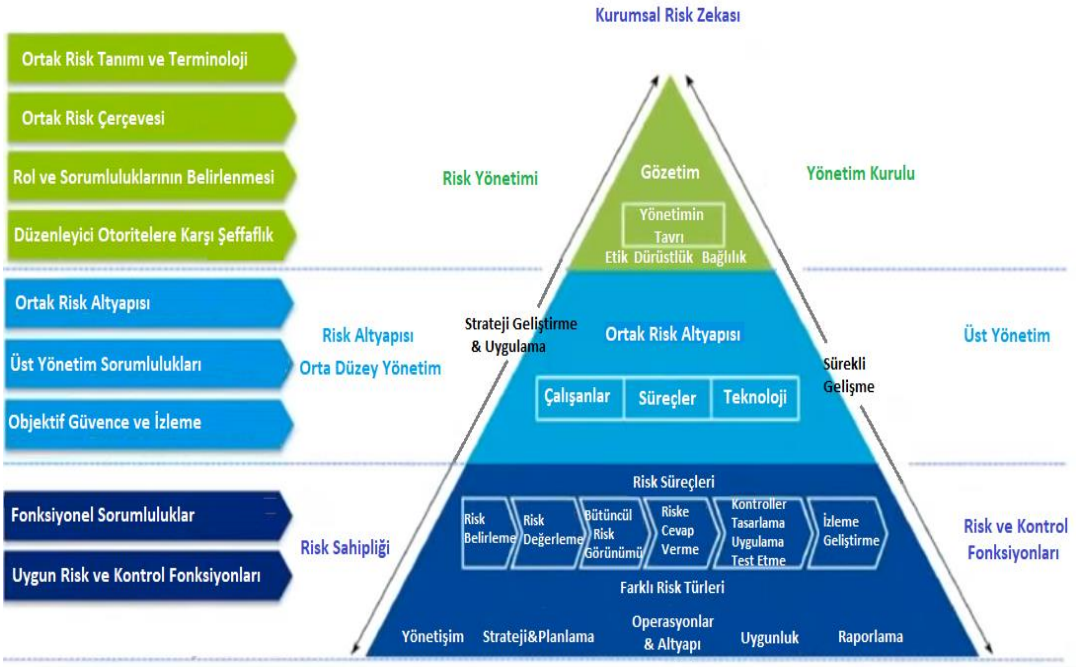
YRU, KRY metodolojisinin de altında bulunduğu bir şemsiye felsefedir. Hem YRU'nun hem de KRY'nin önde gelen amaçlarından biri, işletme kaynakları için en verimli alanları belirlemek amacıyla, işletmenin maruz kaldığı bütün risklerin tespit edilmesini, analiz edilmesini ve ölçülmesini temin etmektir. Hem KRY hem de YRU, riskleri yönetmek ve süreçler arasında işbirliği sağlamak için ortak bir çerçeve sağlar (Banham, 2007, s. 49).

Küreselleşme sonrasında ortaya çıkan yeni ekonomik konjonktür, piyasalarda değişimin ivme kazanması, işletmelerin karşılaştığı yeni zorlukların sayısındaki artış kısacası YRU yaklaşımının ortaya çıkmasının nedenleri olarak sıraladığımız değişimler, kurumsal risk yönetiminin güncellenmesini bir zorunluluk haline getirmiştir. COSO, 2017 yılında çerçevesini, Kurumsal Risk Yönetimi - Strateji ve Performansla Riskin Düzenlenmesi adıyla güncellemiştir. ISO ise, rehberini 2018 yılında ISO31000:2018 Risk Yönetimi Rehberi adıyla yeniden yayımlamıştır. Yapılan güncellemeler incelendiğinde iki rehberde yer alan değişikliklerin, üst yönetimin ve yönetim kurulunun kurumsal risk yönetimine daha fazla dâhil edilmesi ihtiyacını, işletme amaçlarının ve stratejilerinin risk yönetimiyle daha fazla ilişkilendirilmesi gerektiğini ve işletmenin performans değerleme süreçlerinin risk yönetimiyle bütünleştirilmesi gerektiğini vurguladığı anlaşılır.

Her iki rehbere göre, risk yönetimi, işletme fonksiyonlarının birlikte çalışması gereken bir faaliyet haline gelmiştir. İki rehberde, risk yönetimiyle gerçekleştirilen değer yaratma sürecine vurgu yapar ve çalışanlar, süreçler ve teknolojinin düzenlenmesiyle elde edilen risk bilgisiyle donatılmış karar süreçlerinin risk yönetiminin merkezinde yer alması gerektiğini vurgular (Sobel, 2018; IRM, 2018). Risk yönetimini faaliyetlerinin merkezine yerleştiren YRU yaklaşımı, yeni kurumsal risk yönetimi çerçeveleriyle benzer ilkeleri ve yeni çerçevelerde yer alan ilkelerin uygulanabilmesi için gerekli olan benzer örgütsel yapıyı savunur. COSO KRY 2, yeni ISO31000 veya OCEG YRU Modeli 3.0, benzer ilkeleri ve örgütsel yapıyı savunan kurumsal risk yönetimi çerçeveleridir (Hutchins, 2018, s. 7). COSO, ISO ve OCEG çerçeveleri; işletme kültürünün, amaçların, stratejilerin ve performansın risk yönetimiyle bütünleştirilmesi ve üst yönetim, yönetim kurulu ve risk çalışanlarının eşgüdüm ve işbirliği içinde çalışması için gereken uygun örgütsel yapı ve teknoloji altyapısının desteklenmesi konusunda yol gösterir. Şekil 3.13, ister KRY ister YRU olarak isimlendirilsin, risk yönetiminin yönetim kurulu, üst yöneticiler ve risk fonksiyonları tarafından nasıl değer yaratan bir sürece dönüştürüleceğini gösteren yaklaşımın risk yapısını yansıtır.

Risk, organizasyonel performansla yakından ilişkili bir kavramdır. Kurumsal Risk Yönetimi, işletme amaçlarına ulaşılıp ulaşılmadığının anlaşılmasını sağlayan göstergelere dayanarak gerçekleştirilen eylemlerden oluşur. KRY, amaçlara ulaşılması konusunda makul seviyede güvence sağlayabilir (COSO, 2016). YRU, daha iyi iç kontrollerin geliştirilmesi için, risk yönetimi süreçlerinin bütünleştirilmesini sağlayarak, geleneksel kurumsal risk yönetimini genişletmiştir. İşletme yöneticileri, riski etkili ve

verimli bir şekilde yönetmek amacıyla teknolojiden faydalanarak risk yönetimi hakkında çok daha yetenekli hale gelebilirler. Bu durum, örgütsel yapıyla desteklendiğinde, aynı zamanda, daha geniş ve merkezi bir risk görünümü sağlar. Hem YRU hem de yeni KRY yaklaşımının savunduğu, bu yüksek risk yönetimi seviyesi, kurumsal risk zekâsı olarak isimlendirilir (Dittmar & Kobel, 2008; Madlener, 2009, s. 233). Şekil 3.13, YRU yaklaşımının sağladığı Kurumsal Risk Zekâsını gösterir.




**Şekil 3.13.** *YRU Yaklaşımının Sağladığı Kurumsal Risk Zekâsı*

YRU yaklaşımının KRY'nin yerine geçirilmesi her zaman doğru olmaz. Eğer KRY fonksiyonu, yönetişim ve uygunluğa da çözüm üretmez ve bu bileşenleri risk yönetimiyle bütünleştirmezse, YRU girişimini başlatmak en mantıklı çözümdür. Diğer taraftan eğer tersi söz konusuysa, YRU lüzumsuz yere düzgün işleyen sistemi bozmak olacaktır. Zaten bu durumda adı ne olursa olsun, YRU felsefesi işletmede hâkimdir. Ayrıca yönetişim, risk yönetimi ve uygunluk süreçleri için ana bir çerçeve sunan YRU yaklaşımı, risk yönetiminde KRY çerçevesini (Örneğin, COSO KRY) kullanabilir (Clendenen, 2007, s. 50).

### *3.4.2.7. Kurumsal risk yönetiminde iç denetimin sorumlulukları*

Risk yönetiminin önemli araçlarından biri, işletmenin karşı karşıya kaldığı risklerden kaynaklanan zorlukların üstesinden gelirken, amaçlarına ulaşmaya çalışırken veya işletme içinde performansın artırılması yönünde çaba gösterirken önemli seviyede katkı sağlama potansiyeline sahip olan iç denetimdir. İşletme yönetiminin etkin bir risk yönetimi süreci sağlayabilmesinin belki de en sağlam yolu, etkin bir risk yönetimi süreci ve iç kontrol sisteminin ikisine birden objektif güvence sağlayabileceği için iç denetimin uygulanmasıdır. Risk yönetimi alanında iç denetim yoluyla elde edilen danışmanlık, risk analiz sürecinde veya kontrol süreçlerinde destek sunmanın yanı sıra riskin ürettiği etkileri azaltma yöntemlerini belirlemek yoluyla da gerçekleşebilir (Dima, 2013, s. 105-108).

İç denetim, kurumsal risk yönetimi uygulamalarına ilişkin denetimler veya incelemeler yaparak, riske ilişkin sorunların belirlenmesini ve fırsatların değerlendirilmesini destekler. Yönetim kuruluna ve üst yönetime çözüm gerektiren konularda tavsiyelerde bulunmak suretiyle hesap verebilirliği geliştirir. Organizasyonun bağımsız savunma hattını veya başka bir ifadeyle hesap verebilirlik mekanizmasının son hattını (Üç Hatlı Savunma Modeli) oluşturmaktadır. Hesap verebilirliğin son hattını, diğer savunma hatlarından ayıran iki önemli faktör, yüksek seviyede bağımsızlık ve objektiflik ile işletmenin genel olarak tasarımı ve operasyonlarının etkinliği hakkında değerlendirmeler yapabilmesi için yönetime tavsiyeler sunma yetkisine sahip olmasıdır (COSO, 2016, s. 113).

İç denetçiler, risk yönetimi kavramını diğer çalışanlardan daha iyi anlarlar ve değerli öneriler getirebilirler. Bu yüzden iç denetim birimi yöneticisi, etkili risk yönetiminin değeri konusunda yöneticileri ve denetim komitesini eğitirken daha proaktif olmalıdır. İç denetçiler de, bu değeri artırmaya destek olma konusunda rol oynayabilirler. Birçok iç denetim faaliyetinde, yönetimden gelen veriler ve istekler doğrultusunda hazırlanan denetim planları hazırlanırken, risk tabanlı bir model kullanılır. Eğer denetim komitesi ve yönetim, risk yönetimi hakkında güçlü bir anlayışa sahip olmazlarsa ortaya çıkan risk konularını belirleyemez ve bunlara ilişkin uygun faaliyetlere girişemezler. İç denetçiler, denetim komitesi üyelerinin ve yönetimin risk yönetimi anlayışını şekillendirmelidir (IIARF, 2011, s. 8).

Yönetim kurulu ya da dengi bir yönetim organının en önemli ihtiyaçlarından biri, risk yönetimi süreçlerinin etkin bir şekilde çalıştığına ve önemli risklerin kabul edilebilir

bir seviyede yönetildiğine dair güvence sağlamaktır. Güvence, farklı taraflardan alınabilir. Bu güvencenin sağlanması, temel güvence kaynağı olan iç denetim ile tamamlanmalıdır. İç denetim, normal şartlarda üç alanda güvence sağlar (IIA; 2004, s. 4):

- Risk yönetimi süreçlerinin hem tasarımları hem de ne kadar iyi çalıştıkları;
- Kontrollerin ve risklere karşı yürütülen diğer faaliyetlerin etkinliği de dahil olmak üzere önemli olarak sınıflandırılan risklerin yönetimi;
- Risklerin güvenilir ve uygun şekilde değerlendirilmesi, risk ve kontrollerin raporlanması.

Uluslararası İç Denetim Standartları, iç denetçilerin risk yönetimi hakkındaki rol ve sorumluluklarına değinmiştir. Performans Standardı 2100, iç denetim biriminin risk yönetimi ve kontrol süreçlerinin geliştirilmesine yardım ederek ve maruz kalınan riskleri belirleyerek ve değerlendirerek işletmeye destek olması gerektiğini belirtir. Böylece, etkili bir iç denetim, işletmenin uygun kurumsal risk yönetiminin oluşturulmasını kapsayan risk yönetimi süreçlerinin tamamlayıcı parçası haline gelebilir.

Standart 2100'e göre; iç denetçiler, yönetimin uyguladığı risk süreçlerinin yeterliliği ve etkinliğini inceleyerek, değerlendirerek, rapor ederek ve bu konuda iyileştirici önlemler geliştirerek, hem yönetime hem de denetim komitesine yardımcı olmalıdır. Ancak kurumun risk yönetimi ve kontrol süreçlerinden kurum yönetiminin, denetim komitesinin ve yönetim kurulunun sorumlu olduğu unutulmamalıdır. Sadece danışmanlık rolünü üstlenen iç denetçiler risklerin tanımlanması, değerlendirilmesi, risk yönetimi yöntemlerinin uygulanması ve risklerle ilgili kontrol önlemlerinin alınması ve uygulanması konularında yardımcı olabilir (IIA, 2010a, s. 167-168).

İç denetimden risk yönetimi süreçlerinin doğru, tam ve güvenilir bilgi ürettiği hakkında güvence sunması beklenebilir. Güvencenin sağlanması amacıyla risklerin tanımlandığının, değerlendirildiğinin ve raporlandığının tespit edilmesi gereklidir. Risk yönetimi süreçlerinin riskin tanımlanması için faydalandığı araçlar incelenmelidir. Bu araçlar yaygın görülen risk olaylarının listesi, meydana gelmiş risk olayları hakkında araştırmalar, önceden raporlanmış zarar ve kazalar ile iç ve dış denetçilerin keşfettiği bulgulardan oluşur.

İç denetim kontrol ve izleme yordamlarının doğrudan testleri, gözlem, izleme faaliyetlerinde kullanılan bilgilerin yeterliliği testleri ve diğer uygun teknikler ile yönetimin kendini değerlendirme süreçlerinin etkinliğini belirlemelidir. Gregg R.

Maynard iç denetçilerin risk yönetimi için kullanabileceği yolların kısa bir listesini sağlamıştır (Pickett, 2010, s. 224):

- Denetim önceliklerini ortaya koymak için denetim evreninin objektif ve sübjektif bir kombinasyonunu yapın.
- Yönetimin denetim öncesinde belirttiği amaçlarına ulaşma yeteneğini ve yönetimin risk ve tolerans değerlendirmelerini analiz edin.
- İç kontrolleri incelemek için anketler yapın. Üst yönetimi etik standartlar, stratejik planlama ve risk yönetimi açısından analiz edin.
- Risk sınırlarının oluşturulması ve yönetilmesi süreçlerini analiz edin. Belirlenen sınırlar finansal ve operasyonel amaçlara göre ayarlanmış mı?
- Uygunluk ve muhasebe kontrolleri gibi diğer risk yönetimi birimlerini inceleyin. Bu faaliyet, değerlendirmelere güvenilmesini ve riske maruz kalma konusunda büyük resmin anlaşılmasını sağlar.
- Stratejik planlama sürecini ve sonuçlarını gözlemleyin. Karar verme süreci için değil, değişen riskleri denetlemek için gözlem yapın.
- Stratejik girişimleri (örneğin, stratejik ittifaklar ya da yeni projeler gibi) değerlendirin.
- Denetim faaliyetlerini bütünleştirin.
- Denetim sürecinde riske maruz kalmaların net etkisi ve düzeltici kontroller esas alınmalıdır. Denetim tavsiyeleri, riskler kontrollerden az olmalıdır denklemi üzerine kurulmalıdır. Daha sonra, pozisyonu onaylamak için gerekli maddi testlerin kapsamını belirleyin.
- Danışmanlık hizmetleri ve katma değerli bilgi sunarak yönetimle işbirliği yapın.
- Etiği iç kontrolün temel bir unsuru olarak gözden geçirin.
- Risk yönetimi programının kapsamlı bir denetimini yapın.

#### *3.4.2.6.1. Uluslararası iç denetçiler enstitüsünün kurumsal risk yönetimi rehberliği*

1998 yılında IIA tarafından yayınlanan bir mesleki bilgilendirme notu, ilk defa iç denetimin riski yönetme rolünü ele aldı. Bilgilendirme notunda yapılan değerlendirmelere göre, iç denetimin, üst düzey yöneticilerin önemli endişeleriyle yakından bağlantı kurarak ve başarı için önemli görülen konular üzerine yoğunlaşarak organizasyona değer katması gerektiği giderek daha fazla kabul edilmektedir. İç denetçinin sorumlulukları bir yönetim

danışmanının sorumlulukları ile benzerlik gösterir. Verdikleri tavsiyenin teknik kalitesinden sorumludurlar. Ancak durumun kapsamlı bir şekilde anlaşılmasının ışığı altında tavsiyeleri kabul etmek ya da etmemek yönetimin kararıdır. İç denetçilerin, riskin değerlendirilmesine veya kontrollerin tanımlanmasına katılımı aşağıdakileri içerir (Pickett, 2011, s. 84):

- Süreç boyunca üst yönetim ve çalışanlara rehberlik etmek,
- Risk yönetimi çalışma gruplarının bir parçası olmak,
- Üst yönetime risk ve kontrol hakkında uzman tavsiyesi vermek,
- Riskleri ve kontrolleri analiz etmek için iç denetim tarafından kullanılan araç ve tekniklerin doğruluğunu ispatlamak,
- Risk yönetimi için bir uzmanlık merkezi haline gelmek.

1999'da, İç Denetçiler Enstitüsü (IIA), iç denetim tanımını risk yönetimi, kontrol ve yönetişim alanlarında güvence ve danışmanlık faaliyetlerini içerecek şekilde yeniden düzenlendi. Bu tanıma göre, iç denetçilerin risk yönetimi açısından rollerini mutlaka yeniden yapılandırmaları gerekmektedir (Spira & Page, 2003, s. 655). Beş yıl sonra, COSO, kurumsal risk yönetimi için bütünleşik bir çerçeve yayınladı. O günden bu yana, işletmelerde risk yönetimine ilişkin hem güvence hem de danışmanlık hizmetleri sunma konusunda iç denetçilere sorumluluklar yükleyen kurumsal risk yönetimi yaklaşımına doğru küresel çapta bir hareket olmuştur (Zwaan vd., 2011, s. 586-587). COSO Çerçevesi, iç denetçileri, "işletmenin kurumsal risk yönetiminin yeterliliğini ve etkililiğini inceleyerek, değerlendirerek, rapor ederek ve iyileştirmeler tavsiye ederek yönetim ve yönetim kuruluna veya denetim komitesine yardımcı olmaya" yönlendirir. Ancak iç denetimin, geleneksel izleme ve güvence rolünden, tüm sürecin danışmanlık ve genel gözetimini kapsayacak şekilde genişleyen risk yönetimi fonksiyonundaki sorumlulukları, tamamen benimsenmedi ve genellikle tam olarak anlaşılamadı. Birçok organizasyon, risk yönetimi yaklaşımında, iç denetimin kullanımında aşırı uçlara gitti. Bazı işletmeler, iç denetim bölümlerini, iş riskleri üzerinde sorumluluk almaya ve bazıları da iç denetçileri sıkı bir izleme rolünü üstlenmeye zorladı (Hall, 2007, s. 4).

İç denetim, KRY faaliyetlerinde organizasyona değer katarken, bağımsızlık ve objektifliğinden ödün verme riskiyle karşı karşıyadır. Bu olasılığı göz önüne alarak, 29 Eylül 2004'te IIA, COSO çerçevesinin yayımlanmasına yanıt olarak IIA-İngiltere ve İrlanda üyeleri tarafından hazırlanan "Kurumsal Risk Yönetiminde İç Denetimin Rolü" başlıklı raporunu yayımladı. Bu rapor, iç denetçilerin risk yönetimi süreçlerine güvence

ve danışmanlık hizmetleri sunarken, IIA'nın profesyonel standartlarının gerektirdiği objektifliği ve bağımsızlığı sürdürebilmelerinin yollarını göstermiştir. Rapor, iç denetim işlevinin KRY süreci boyunca dahil olması ve olmaması gereken rollerini belirlemiştir. KRY ile ilgili temel iç denetim sorumlulukları, belirli şartlar altında iç denetimin üstlenebileceği meşru sorumluluklar ve iç denetimin üstlenmemesi gereken sorumluluklar başlıkları altında 18 faaliyet tanımlanmıştır (Bkz. Tablo 3.4) (Hall, 2007, s. 4).

**Tablo 3.4.** *Kurumsal Risk Yönetiminde İç Denetimin Rolü (IIA, 2004, s. 4)*

| | |
|---|---|
| **İç Denetimin Kurumsal Risk Yönetimine İlişkin Temel Sorumlulukları** | Risk yönetimi süreçlerine güvence sağlanması<br>Riskin doğru değerlendirildiğine ilişkin güvence sağlanması<br>Risk yönetimi süreçlerinin değerlendirilmesi<br>Temel risklerin uygun şekilde raporlanıp raporlanmadığının değerlendirilmesi<br>Temel risklerin üst yönetim tarafından yönetilip yönetilmediğinin incelenmesi |
| **İç Denetimin Kurumsal Risk Yönetimine İlişkin Belirli Şartlar Altında Üstlenebileceği Meşru Sorumlulukları** | Risklerin belirlenmesinin ve değerlendirmesi sürecinin kolaylaştırılması<br>Risklerin tanımlanması ve değerlendirilmesinde üst yönetime rehberlik edilmesi<br>Kurumsal Risk Yönetimi faaliyetlerinde koordinasyonun sağlanması<br>Risklere ilişkin konsolide raporlar hazırlanması<br>Kurumsal Risk Yönetimi çerçevesinin devamlılığının ve gelişiminin sağlanması<br>Kurumsal Risk Yönetimi yaklaşımının benimsenmesinin desteklenmesi<br>Yönetim kurulunun onayına sunulacak risk yönetim stratejisinin geliştirilmesi |
| **İç Denetimin Kurumsal Risk Yönetimine İlişkin Üstlenemeyeceği Sorumluluklar** | Risk iştahının ayarlanması<br>Risk yönetimi süreçlerinin düzenlenmesi<br>Riskler hakkında üst yönetimin çalışmalarında etkinliğinin garanti edilmesi<br>Risklere karşı yapılacak eylemlerin belirlenmesi<br>Risklere yönelik yapılacak eylemlerin yönetim adına uygulanması<br>Risk yönetimi sorumluluğunun üstlenilmesi |

İç denetçilerin KRY'deki rollerinin belirlenmesinin sebebi, bağımsızlığının ve objektifliğinin zarar göreceği endişesidir (Zwaan vd., 2011, s. 588). İç denetim birimi yöneticisi bu endişesini gidermek için, birim faaliyetlerinin kapsamına iç denetim tüzüğünde yer vermeli ve denetim komitesine onaylatmalıdır. İç denetimin yönetim adına riskleri yönetemeyeceği, sadece karar verme sürecine tavsiyelerde bulunacağı ve güvence hizmetleri dışındaki her faaliyetin danışmanlık hizmeti kapsamında değerlendirileceği deklare edilmelidir (Reding, 2013, 4-18). Ayrıca iç denetimin bir yönetim sorumluluğu üstlenmediğinin belirlenmesi, güvence sorumluluklarının danışmalık hizmetiyle uyumlu olup olmadığına karar vermede belirleyici bir unsurdur (Maytjewicz & D'arcangelo, 2004, s. 10).

Bir işletmede risk yönetim uzmanının ya da biriminin faaliyetlerinden yararlanıldığında, iç denetim biriminin danışmanlık faaliyetlerine girmektense güvence rolü üzerine yoğunlaşması, işletmeye değer katması olasılığını artırır. Benzer şekilde güvence faaliyetlerinin gerektirdiği risk bazlı yaklaşım benimsenmeden, iç denetimin danışmanlık rolünü üstlenmek için gerekli olan donanıma sahip olduğu söylenemez.

İç denetimin kurumsal risk yönetimine dair güvence rolünün dışında bir takım faaliyetlerde bulunması, işletmeden işletmeye farklılık gösterir. İşletmede risk yönetimi, işletme faaliyetleriyle bütünleştikçe, iç denetimin destek verici rolü azalabilecektir. Benzer şekilde, işletmede risk yönetimi fonksiyonu için uygun bir ekip oluşturulmuşsa, iç denetim danışmanlık hizmetlerinden ziyade, güvence hizmetlerine odaklanmalıdır (Bozkurt, 2010, s. 24-25).

IIA rehberliği, iç denetçiler belirli şartlar altında üstlenilebilecek iç denetim sorumlulukları olarak tanımladığı meşru danışmanlık faaliyetlerini üstlendiğinde, riskleri gerçek anlamda yönetmek için yönetim sorumluluğunu üstlenmediklerini garanti altına alacak önlemlerin alınması gerektiğine dikkat çekmektedir. Muhtemel bir tedbir, denetim komitesinin onayladığı iç denetim yönetmeliğinde, denetçilerin KRY sorumluluklarının belgelendirilmesidir. Ayrıca, denetçiler bu danışmanlık rolüne giren herhangi bir KRY ile ilgili faaliyette bulunursa, bu görevleri danışmanlık görevleri olarak değerlendirmeli ve bağımsızlık ve nesnelliğini sağlamak için ilgili IIA standartlarını uygulamalıdırlar (Gramling & Myers, 2006, s. 55). İç denetim biriminin KRY hakkındaki görevlerini genişletebilmesi için gerekli olan şartlar şunlardır:

- Risk yönetiminden üst yönetimin sorumlu olduğu açıkça ortaya konmalıdır.
- İç denetimin sorumluluklarına doğası gereği iç denetim yönetmeliğinde açıkça yer verilmeli ve denetim komitesi tarafından onaylanmalıdır.
- İç denetim, yönetim adına herhangi bir riski yönetmemelidir.
- İç denetim birimi risk yönetimi kararlarını kendisi almamalı, yönetimin karar alma sürecine tavsiyelerde bulunmalı ve destek olmalıdır.
- İç denetim KRY çerçevesinin sorumlu olduğu herhangi bir bölümüne güvence veremez. Böyle bir güvence diğer uygun nitelikteki kesimler tarafından sağlanmalıdır.
- Güvence faaliyetlerinin dışındaki herhangi bir görev, danışmanlık işlevi kapsamında görülmeli ve buna göre uygun uygulama standartlarına uyulmalıdır.

İç denetimin KRY'de asli rolü, risk yönetiminin etkinliğine dair yönetim kurulu ve üst yönetime güvence sağlamaktır. İç denetçi asli rolünün ötesine geçerek danışmanlık hizmetleri sunmaya başladığında, IIA'nın belirlediği önlemleri alarak ve standartlara azami dikkat göstererek bağımsızlığını ve objektifliğini korumak zorundadır. Bu sınırlamalara özen gösterildiğinde KRY, iç denetim biriminin işletme içinde daha etkin bir konuma ulaşmasına katkı sağlayabilir (IIA, 2009, s. 6).

IIA Standartları, denetledikleri faaliyetlerle ilgili olarak hangi rollerin iç denetçilerin tarafsızlığını açıkça koruyan uygun faaliyetler olduğunu gösterir. Objektiflik, iç denetçilerin konumuna, yetkilerine ve uygun iç denetim çalışanlarının atamalarına yansıtılmalıdır. Uygun konum ve yetkilendirme; denetimin kapsamı ve değerlendirilmesi için yeterli yetkiye sahip bir şahsa raporlama yapılması, CAE'nin seçilmesi ve görevden alınmasının ancak yönetim kurulu ve denetim komitesinin mutabakatı ile mümkün olması; yönetim kuruluna veya denetim komitesine açık erişimin sağlanması gibi düzenlemelerin yapılmasını gerektirir (COSO, 2004, s. 88).

İşletme dünyasında değişen risk faktörleri ve ortaya çıkan riskler, iç denetimi risk yönetimi faaliyetlerini genişletme yönünde zorlamaktadır. Yeni COSO çerçevesi ve güncellenen ISO 31000 rehberi, risk yönetimi faaliyetlerinin kapsamının bütüncül bir bakış açısıyla genişletilmesi gerektiğini savunur. İç denetçilerin risk yönetimi sorumluluklarının sınırlarını, görevlerini genişletebilmesi için gerekli olan şartları dikkate alarak, mümkün olan en üst seviyeye taşıması gereklidir. İç denetim standardı 2120, halihazırda daha fazla görev alınmasına meşruiyet kazandırır. 2120'ye göre; "*iç denetim faaliyeti, risk yönetimi süreçlerinin etkinliğini değerlendirmeli ve iyileştirilmesine katkıda bulunmalıdır*." Zaten Standart 2010'da ifade edilen, "*iç denetimin önceliklerini belirlemek için organizasyonun amaçlarıyla tutarlı risk bazlı bir plan oluşturması*", ancak etkin işleyen KRY'den elde edilen çıktılarla gerçekleştirilebilir. İç denetim aşağıdaki faaliyetleri mümkün olduğunca üstlenmeye çalışmalıdır (COSO, 2016; Herron & Dholabhai, 2017; Sobel, 2018):

- Risklerin bütünleşik görünümünü sağlamak amacıyla iç denetim ve KRY ortak risk değerlendirme faaliyetleri yapmalıdır.
- Yönetimin eylem planları doğrulanmalı ve planlanan ilerleme değerlendirilmelidir.
- KRY süreçlerinin olgunluğu ve etkinliği değerlendirilmelidir.
- Seçilen stratejilerin riskleri konusunda daha güçlü bir bakış açısı sağlamak için strateji belirleme tartışmalarına katılmalıdır.

- Yüksek riskli alanlarda daha fazla denetim süreçleri ve kontroller geliştirilmelidir.
- Organizasyonun risk iştahı gözden geçirilmelidir.
- İşletmenin nasıl değer yarattığı ve koruduğu anlaşılmalıdır.
- Risk ve kontrol fonksiyonlarının çalışanları ortak iş dili ile senkronize çalışmaya teşvik edilmelidir.
- İşletme içinde risk farkındalığı artırılmalı, işletme örgütün KRY'yi bir fonksiyon, birim ya da bağımsız bir araç değil, bir süreç olarak görmesi sağlanmalıdır.

Herhangi bir yönetim sorumluluğu üstlenmemesi koşuluyla, iç denetim faaliyetinin risk yönetimine daha fazla katkı sağlama potansiyeli vardır. Risk yönetimine güvence sağlamanın yanında, iç denetim risk yönetiminin anlaşılması ve koordine edilmesi konusunda danışmanlık yapabilir. Bu bağlamda iç denetçiler, risk yönetimi süreçlerinde çerçeve, teknoloji ve araçların kullanılması için tavsiyelerde bulunmalı ve süreçlerin oluşturulması ve sürdürülmesi için politika ve yordamlar geliştirilmesine katkı sağlamalıdırlar (Adams vd., 2016, s. 94). Teknoloji, herhangi bir risk yönetim programı için önemli bir etkinleştirici olabilir. Birçok işletme, toplanan verileri yönetmek, izleme faaliyetlerini yürütmek ve iletişim zorluklarını ortadan kaldırmak için bir teknoloji çözümüne ihtiyaç duyduğunun farkına varacaktır. Bununla birlikte, bir teknoloji çözümü seçmeden önce, risk yönetimi yaklaşımını oluşturmak önemlidir. Aksi takdirde işletme, ihtiyaçlarına ve kültürüne daha iyi uyan bir yaklaşım yerine tedarikçinin dayattığı yaklaşımı benimsemek zorunda kalabilir.

#### *3.4.2.6.2. Kurumsal risk yönetiminin iç denetim faaliyetlerine etkisi*

Beasley, Clune ve Hermanson (2005) tarafından iç denetçiler üzerinde anket yoluyla yapılan çalışma sonucunda, KRY'nin iç denetim üzerinde üç önemli etkiye yol açtığı sonucuna varılmıştır:

- KRY iç denetimin işletme risklerini daha iyi anlamasına neden olmuştur, böylece iç denetim planları ve testlerini etkilemiştir.
- KRY iç denetimin işletme içinde daha etkili bir statüye sahip olmasını sağlamıştır.
- KRY iç denetimin iş yükünü artırmıştır.

Risk yönetimi çerçevesini ve süreçlerini geliştiren ve uygulayan önde gelen işletmelerde iç denetim, risk yönetimi alanında bir ortak olmayı başarmıştır. Bu ortaklığın tesis edilebilmesi için iç denetimin (Selim & McNamee, 1999, s. 159);

- Riskin belirlenmesi ve anlaşılması süreçlerinde risk yönetimine katılması,
- Stratejik süreçler ve riskler arasında ve operasyonel süreçler ile riskler arasında önemli bağlantıları kurması,
- Stratejik planlar ile denetim evreni ve operasyonel iş planları ile yıllık denetim planları arasındaki gerekli iletişimi öne çıkarması,
- Denetim paradigmasını kontrol temelli denetimden risk temelli denetime dönüştürmesi gereklidir.

Ortak bir çerçevenin ve ortak bir risk dilinin varlığı, risk yönetimi ilkelerini bütünleştiren organizasyonların en önemli ayırt edici özelliklerinden biridir. Yöneticiler, risk unsurlarını anlamak için bir model veya çerçeve kullanırlar. Ortak bir dil ve kavramlar setini paylaşarak, işletme içinde tüm birimlerden yöneticiler, belirsiz bir işletme çevresinde işletmeyi yönetmelerine yardımcı olmak için bilgiyi tartışabilir ve ona katkıda bulunabilirler. İç denetim uygulanırken, risk değerlendirmesi üç önemli unsuru gerektirir (Selim & McNamee, 1999, s. 167):

- Risklerin değerlendirildiği iş sürecinin kapsamlı bir şekilde anlaşılması;
- Riski tartışmak için bir çerçeve ve ortak dil;
- Var olabilecek risklerin ve fırsatların doğası hakkında düşünebilmenin teşvik edilmesi.

Risk tabanlı denetimin amacı, etkisi yüksek alanlara odaklanarak, denetim kaynaklarının işletmenin önceliklerine göre kullanılmasıdır. IIA Uygulama Standartlarına göre, iç denetim yöneticisi işletmenin amaçlarına uygun olarak, iç denetim faaliyetinin önceliklerini belirleyen çalışma planları yapmalı ve bu planlar yılda en az bir defa yapılan risk değerlemesini referans almalıdır. Risk değerleme süreci sayesinde, iç denetim reaktif ve kontrole dayalı olmaktan çıkıp, proaktif ve riske dayalı bir hale gelir. Etkin risk değerleme sayesinde iç denetim, mevcut sorunlara çözüm getirmenin yanında, olayların önceden farkına vararak işletmeyi ortaya çıkabilecek zararlardan korur ve fırsatların yakalanmasına katkı sağlar (Eşkazan, 2005, s. 33).

İç denetimdeki risk değerleme, bir denetimin denetlenebilir alanlar üzerinde yoğunlaşması için riskleri tanımlar, önlemleri alır ve önceliklendirir. Bir denetimde, denetçi, denetim kapsamındaki en önemli alanları belirlemek için risk değerleme yapar. Risk değerleme, denetçinin, en önemli kontrolleri veya denetimleri daha derin veya daha ayrıntılı olarak test eden bir denetim programı tasarlamasına izin verir. Risk tabanlı denetim, bu modeli genişletir ve geliştirir (Selim & McNamee, 1999, s. 168).

Denetim faaliyetinin odak noktasının, geçmişteki faaliyetlerden geleceğin yönetilmesine dönüşümünün günümüzdeki ifadesi risk odaklı iç denetimdir (Kurnaz & Çetinoğlu, 2010, s. 84). Diğer bir ifadeyle, işletmenin risk profilinin tespit edilmesi, denetim sürecinin bu profile göre şekillendirilmesi ve denetim etkinliğini arttırmak amacıyla denetim kaynaklarının nispeten riskli alanlara harcanması esasına dayanan bir yaklaşımdır (Özsoy, 2004, s. 1).

Risk odaklı denetim, işletme için daha fazla sorun yaratan alanların denetlenmesini amaçlayan bir süreç, bir yaklaşım, bir metodoloji ve aynı zamanda bir tutumdur. Hangi konular gerçekten problem yaratır? Bu sorunun yanıtı, büyük olasılıkla yüksek risk taşıyan işletme unsurları olacaktır. İşletme için önem taşıyan riskli unsurlar, aynı zamanda denetim faaliyeti için tespit edilmesi gereken temel unsurlardır. İşletmede kurumsal risklerin tanımlanması ve değerlendirilmesi sürecinde iç denetçi, yönetimle işbirliği yapmalıdır (Griffiths, 2005 s. 5).

Denetim önceliklerini oluşturmak, iç denetim biriminin önemli bir işlevidir. Risk yönetimi faaliyetleri ile ilgili olarak, iç denetçilerin kontrollerin test edilmesi için öncelikleri belirlemesi gereklidir. Risk yönetimi ve iç kontrol arasında önemli bir bağlantı vardır. Risk yönetimi uzmanları, riskleri değerlendirmede ve kurulması gereken uygun kontrolleri belirleme konusunda uzmandır. Risk yönetimi genellikle mevcut kontrolleri kaydeder ve ek kontrollerin uygulanması için tavsiyelerde bulunur. İç denetçinin temel işi bu noktada başlar. Kritik önem taşıyan kontrolleri tanımladıktan sonra, iç denetçi, doğru ve etkili kontrollerin uygulamaya konulduğunu kontrol etmelidir. Kontrol testlerinin sonucunda, amaçlanan risk düzeyinin uygulamada gerçekten elde edilmesi sağlanır. Bir başka deyişle kontrol, risk seviyesini, önceden planlandığı gibi tespit edilen seviyeden istenen seviyeye taşır. Kontroller konusundaki sorunlar, risk yönetimi ve iç denetim tarafından giderilmeye çalışılsa bile, kontroller üzerindeki nihai kararlar ve kontrollerin beklenen etkinliği, kontrollerden sorumlu olan üst yöneticiler tarafından belirlenmelidir (Hopkin, 2010, s. 303).

Bir işletmenin varlığını sürdürebilmesi, müşteri ihtiyaçlarına cevap verebilmesine ve faaliyetlerinde başarılı olmasına bağlıdır. İşletmenin bunu gerçekleştirebilmek için, etkin işleyen iş süreçlerine sahip olması ve bunları zamanla değişen şartlara veya ortaya çıkan aksaklıklara karşı güncellemesi gereklidir. Aksi durumda maddi kayıplarla karşılaşılabilir veya hatalı kararlar alınabilir. İç denetimin işletmeye yaptığı ekonomik fayda, iç kontrolün etkinliği ve yerindeliğini değerlendirerek ve yöneticilere risk yönetimi

konusunda katkı sağlayarak iş süreçlerinde verimliliği artırmak ve risklerin yol açtığı kayıpları engellemektir (TÜSİAD, 2008, s. 7).

#### *3.4.2.6.3. Kurumsal risk yönetiminde iç denetim birim yöneticisinin sorumlulukları*

Risk yönetiminde sorumluluğun üstlenilmesi ile risklerin yönetilmesi için örgütsel yeteneklerin ve araçların geliştirilmesi birbirinden ayrılır. İç denetçiler, belirli koşulların sağlanması halinde örgütsel yeteneklerin ve araçların geliştirilmesi faaliyetleriyle uğraşabilirken; risk yönetiminde sorumluluk üstlenilmesi bağımsızlığı zedeleyeceği için asla kabul edilemez (Adams, 2016, s. 92). IIA, risk yönetiminde esas sorumluluğun üst yönetimde olması gerektiğini açıkça ifade etmiştir. İç denetçi, yönetimin risk yönetimine ilişkin kararlarını incelemeli, gerektiğinde destek olmalı ve öneriler getirmelidir. Ancak risk yönetimi kararlarını bizzat almamalıdır. İşletmede iç denetimin risk yönetimine ilişkin sorumlulukları hakkındaki belirsizlik, söz konusu sorumlulukların denetim komitesince onaylanmasıyla giderilebilir (Kara & Sakarya, 2012, s. 77).

İç denetçiler, risk yönetiminde önemli rol oynayabileceklerini ancak iç denetimin risk yönetimi faaliyetlerini takip etmeye hazır olmadığını veya takip etmeye yönelik proaktif bir yapıya sahip olmadıklarını düşünmektedirler. Genel olarak iç denetim fonksiyonları, risk yönetimi odaklı bir yaklaşımı benimsemek zorundadırlar. Özellikle, iç denetim birimi başkanlarının, risk yönetimi konusunda aşağıdakileri yapmaları için fırsatları vardır (IIARF, 2011, s. 5):

- Risk ve risk yönetimi kavramları hakkında denetim komitelerini ve yönetimi eğitmek,
- Risk Yönetiminde İç Denetimin Rolü başlıklı IIA Pozisyon Belgesinde tanımlanan temel iç denetim sorumlulukları hakkında işletme çapında güvence sağlamak,
- KRY yöneticilerine daha fazla risk yönetimi danışmanlığı hizmeti sunma fırsatlarını araştırmak ve bu danışmanlık hizmetlerinin sonuçlarını resmi olarak denetim komitesi ve yönetimle paylaşmak,
- Yönetimin (1) önemli stratejik riskleri kapsamlı bir şekilde tanımlayıp tanımlamadığını, (2) bu riskleri gidermek için ihtiyatlı risk yönetimi teknikleri geliştirmiş olup olmadığını ve (3) zamanında ve uygun eylemler geliştirmek için riskli olayları belirleyen stratejik risk işaretlerinin yeterince izlenip izlenmediğini değerlendirmek,

- İç denetim ekiplerinin risk yönetimi ile ilgili doğru seviyede beceri ve tecrübeye sahip olması için yeterli seviyede zaman, kaynak ve liderliği ayırmak,
- İç denetim faaliyetinin risk yönetimi becerilerine katkı sağlamak için iç ve dış kaynakları kullanmak.

Risk tanımlamanın doğru yapıldığının yanı sıra iç denetçiler, artık risk seviyelerinin doğru anlaşılması ve değerlendirilmesi amacıyla risk olaylarını incelemelidirler. Risk seviyelerinin değerlendirilmesi ve raporlanması süreçlerinin doğru yapıldığından emin olmalıdırlar. İç denetçiler, bu şekilde risk yönetimine ilişkin bir görüş oluşturabilirler. Risk yönetimi hakkında görüş oluştururken, iç denetçilerin cevabını aradıkları başlıca sorular şunlardır: Önemli riskler tanımlanmış ve değerlendirilmiş mi? Risklere karşı gereken önlemler alınmış mı? Risklere karşı geliştirilen eylemlerin kabul edilebilir sonuçlar doğurma ihtimali nedir? Ayrıca iç denetçilerin risk yönetimi kararlarını incelemelerinde temel endişelerinden biri de, riske ilişkin kararların yetkili kişiler tarafından alınıp alınmadığıdır (Adams, 2016, s. 93). İşletmelerinde KRY'ni teşvik etmek isteyen iç denetim birimi başkanları için aşağıdaki faaliyetler sürecin başlatılması için yardımcı olabilir:

- İç denetim çalışanlarıyla KRY'ni tartışmak için bir toplantı düzenleyin.
- İşletmeniz için KRY'nin durumunu ve iç denetimin olası KRY rolünü resmi olarak değerlendirmek için iç denetim içinde bir proje ekibi atayın.
- Gerekirse başlangıçta eğitime odaklanan bir KRY tartışmasını denetim komitesine taşıyın.
- KRY'nin benimsenmesi ve iç denetimin KRY'deki rolü için üst yönetim ve denetim komitesinin desteğini alın.

### 3.4.3. Uygunluk

Uluslararası, siyasi ve çevresel girişimleri desteklemek amacıyla yakın zamanda yürürlüğe konan çok sayıda yasal düzenleme ve bunların ihlali halinde önemli cezalar ve yaptırımlar ile karşılaşılması, günümüzde özellikle uluslararası ticarette özel bir endişe kaynağı haline gelmiştir. Son beş yılda yasa ve düzenlemelerin sayısında çok büyük bir artış yaşanmış, üstelik mevzuattaki değişimin hızı takip edilemeyecek hale gelmiştir (Lynford, 2015, s. 61).

Uygunluk günümüzde yönetim kurullarında strateji ve risk yönetimiyle birlikte tartışılmaya başlanmıştır. Önemli maliyet artışlarının yanı sıra etkinliğe ve verimliliğe

odaklanmak, uygunluğun tartışılması için iyi bir nedendir. Yöneticiler, işletmelerinin tabi olduğu sayısız kanun ve yönetmeliği iyi bilmelidir. Ürün güvenliği, istihdam, işyerindeki sağlık ve güvenlik, çalışanların menfaatleri, emeklilik aylığı, borsa düzenlemeleri, bilgi gizliliği, para aklamayla mücadele, ürünün müşteri profiline uygunluğuyla ilgili özel düzenlemeler ve sağlık hizmetleri, tütün ve telekomünikasyon şirketleri için sanayiye özgü sınırlamalar birçok farklı sektördeki işletmenin uymakla yükümlü olduğu yasa ve düzenlemelere örnek gösterilebilir (Steinberg, 2011, s. 24).

Her işletme, kuruluş ve faaliyetleri için geçerli olan yasa ve yönetmeliklere uymaya çalışmalıdır. YRU kısaltmasında U, uygunluğu ifade eder. İşletmeler yasa ve düzenlemelere uyum sağlamanın maliyetlerinin giderek yükseldiğinin ve çoğu zaman milyonlarca dolara ulaşan para cezalarının ve faaliyet sınırlamalarının etkinliği azalttığının farkına varmışlardır. Her yeni yasa ve düzenlemeyle birlikte politikalar ve yordamlar oluşturulabilir, ancak bunlar benzeşmez, birbirini tekrar eder ve etkili bir uygunluk programının oluşturulmasında başarısızlığa neden olur.

Buna karşın uygunluk programlarını etkili ve verimli hale getiren işletmeler, çok büyük iş kazançları elde edebilirler. Sürekli genişleyen hukuki ve düzenleyici gerekliliklerin gerekçelerinin anlaşılması, pazarı yönlendiren temel nedenlerin farkına varılması ve pazar payı, kâr ve kazanç elde etmek için stratejik girişimlerin şekillendirilmesi uygunluktan elde edilen faydaları ortaya çıkaran temel faktörlerdir. İşletme amaçlarını düzenlemek ve uygunluk programlarını mevcut yönetim ve iş süreçlerine yerleştirmek suretiyle, sorumluluk ve hesap verebilirlik en uygun iş seviyesine yerleştirilir, verimlilik arttırılır, maliyetler azaltılır ve üst yönetim ve yönetim kuruluna ihtiyaç duydukları bilgi sağlanır (Steinberg, 2011, s. 21).

İşletmelerin çoğunun sahip olduğu, sadece yasa ve düzenlemelerin acil gereksinimlerini yerine getirmeye çalışan uygulama yaklaşımları, bütünleşik bir yaklaşım benimsenmediği için yetersiz kalacaktır. Bu yaklaşımın, işletmelere getirdiği yüklerden en önemlisi yasa ve düzenlemelerin maliyetlerinin kontrol edilemez hale gelmesidir. İşletme uzmanları ve danışmanlar, çok farklı kaynakların dayattığı, karmaşık ve çok sık değişen mevzuata ve işletmenin kendi belirlediği politika ve yordamlara uymak için bütünleşik bir uygunluk yönetimi yaklaşımının gerekli olduğunu savunmaktadır. Bütüncül bir uygunluk yönetimi, YRU yaklaşımını gerektirir (Bonazzi vd., 2009, s. 392).

İşletmelerin uygunluk programı konusunda çalışanları ve paydaş grupları ile iletişim kurması karmaşık ve zordur. Danışmanlar ve mesleki ticaret örgütleri, uygunluk

programlarına ilişkin çeşitli yaklaşım, çerçeve ve modellere sahiptir. Bu modeller, uygunluğun diğer ilişkili disiplinler ve birçok değişkenden bağımsız ele alınmaması gerektiğini savunur. Uygunluk, yönetişim ve risk yönetimi (YRU kısaltmasıyla ifade edilmiştir) ile birlikte ele alınmalıdır. Uygunluğu, bu iki disiplinden ayırmak çok zordur. Uygunluk yönetimi YRU'daki U'ya odaklansa da, bu üç alan kavramsal olarak ve uygulamada birbirine çok sıkı bir şekilde bağlı olduğundan, diğer iki alandan bağımsız olarak uygunluğu ele almak tam anlamıyla mümkün değildir. Bunun nedeni, yönetişimin, risk yönetiminin ve uygunluğun her bir öğesinin ayrı olarak görülemeyecek ve görülmemesi gereken örgütsel faktörleri, insanları, süreçleri ve teknolojileri kapsamasıdır. Bu nedenle yönetişim ve risk yönetiminin etkili bir uygunluk programında derinlemesine yer aldığı akıldan çıkarılmamalıdır (Kral, 2009, s.3).

Uygunluğu, risk ve yönetişim ile bütünleştirmek için tasarlanan bazı çerçeveler vardır ve son dönemde birçok işletme tarafından uygulanmaktadır. Bunların en önemli ve kapsamlılarından biri Açık Uygunluk ve Etik Grubu'nun yayımladığı YRU Yetenek Modelidir (Ghiran & Bresfelean, 2012, s. 754).

#### *3.4.3.1. Uygunluk kavramı*

Açık Uygunluk Etik Grubunun yaptığı tanıma göre uygunluk, yasalar ve düzenlemeler tarafından tanımlanan zorunlu gerekliliklere ve sözleşme yükümlülüklerinden ve iç politikalardan kaynaklanan gönüllü gerekliliklere bağlı kalarak hareket etmeyi ve bağlı kalmak için sahip olunması gereken yeteneği ifade eder (OCEG, 2009, s. 9).

Genel olarak, uygunluk sizin için belirtilen bir koşullar setine cevap verebiliyor olmanız anlamına gelir. Uygunluk, başka birisinin sizin için koşullar düzenlediğini ve sizin bu koşullara uymanız gerektiğini belirtir. Çoğu zaman, insanlar uygunluk hakkında konuşurken, zorunlu olarak uyulması gereken dış standartları kastederler. Ancak uygunluk kelimesi bazen iç standartlara uyumu da yansıtır (Broady & Roland, 2008, s. 23).

Açık ve sade bir şekilde ifade etmek gerekirse, uygunluk kavramı; yasalar, düzenlemeler, protokoller ve standartlar uyarınca hareket etmektir. Uygunluk hakkındaki asıl mesele; adli, finansal, şirket itibarıyla ilişkili ve piyasa şartlarının yol açtığı uyumsuzluğun maliyeti etrafında dönmektedir. Uygunluk, yasama organları tarafından yürürlüğe sokulan yasalara, politikalar ve yordamlar gibi iç gerekliliklere ve düzenleyici

kurumlar tarafından oluşturulan düzenlemelere uyum sağlamayı kapsar (Tarantino, 2008, s. 21).

#### *3.4.3.2. Uygunluğun önündeki engeller*

Günümüzün sürekli değişen işletme çevresinde, işlemelerin hem zorunlu hem de gönüllü gerekliliklerine uyum sağlamasının önünde bazı engeller vardır. Bunlar şöyle sıralanabilir (Eggert, 2014, s. 8; Moeller, 2011, s. 26):

- Yasalar ve düzenleyici otoriteler tarafından sık sık yeni düzenlemeler getirilmesi,
- İşletmenin uyması gereken düzenlemelerin yorum getiren, belirsiz ifadeler içermesi,
- Uygunluğun sağlanması ve sürekli olarak izlenmesi için geliştirilen iç kontroller hakkında, birimler arasında fikir birliğine ulaşılamaması,
- İşletmede uygunluk kültürünün olmaması,
- Yüksek maliyetler,
- İşletmede etkili risk yönetiminin olmaması,
- Uygunluk belgelerinin oluşturulmasının zorluğu,
- Uygunluğun katma değer yaratan bir eylem olarak algılanmaması,
- Yasa, düzenleme ve politikaların işletme faaliyetleriyle ilişkilendirilmesinin zorluğu,
- Çalışanlar arasında iletişimin olmaması,
- İşletmenin uyması gereken birçok düzenlemenin aynı konularla ilgili kurallar getiriyor olması,
- Uyulması gereken düzenlemelerin sık sık değiştirilmesi veya güncellenmesi.

#### *3.4.3.3. Uygunluk başarısızlıklarına neden olan faktörler*

Deneyimli yöneticiler, büyük bir uygunluk başarısızlığının yalnızca milyarlarca dolar doğrudan maliyetle karşılanamayacağını aynı zamanda bir işletmeyi çok daha karmaşık sorunlarla karşı karşıya bırakacağını iyi bilir. Bu başarısızlıkların minimum etkisi, üst yönetimin zamanını ve enerjisini azaltması, şirketin günlük işleyişini sekteye uğratması ve işi büyütmek için yapılması gereken yeni girişimlerin etkinliğini azaltmasıdır. Bu başarısızlıklar müşteriler, tedarikçiler, ortaklar, bankacılar ve yatırımcılar ile olan ilişkileri bozar, geliştirilmesi yıllar alan şirket itibarını bir gecede

mahveder, kilit insan kaynaklarının muhafaza edilmesini engeller ve sonuç olarak uzun vadeli başarıyı tahrip eder. İşletmelerin uygunluk başarısızlıklarıyla karşı karşıya kalmalarına yol açan bir konuma gelmelerine neden olan bazı faktörler şöyle sıralanabilir (Steinberg, 2011, s. 31):

- İşletmeler genellikle davranış kuralları, ihbar kanalları ve eğitim programlarından oluşan yasa ve düzenlemelere uymaya yönelik bir dizi politika ve yordama sahiptir. Bazı büyük şirketlerde sektöre bağlı olarak belirli bir uygunluktan sorumlu yönetici ve personel bulunurken diğerlerinde genel hukuk danışmanı veya diğer kurumsal avukatlar rol almaktadır. Fakat çoğu zaman bunlar, gerçek bir uygunluk programı oluşturarak etkili bir şekilde çalışamayan farklı unsurlardır.
- Her biri yasa ve düzenlemelerin dayattığı gerekliliklerin çeşitli yönlerini etkileyen politika ve yordamlar genellikle birbirleriyle ortak bazı eylemlerin olduğu bir katman oluşturur. Her yeni yasa veya yönetmelik için, yeni iç politikalar ve yordamlar yasaların özelliklerini ele almak üzere tasarlanmıştır. Maalesef, her biri genellikle yeni gereksinimleri karşılayabilecek mevcut protokollere bakılmaksızın oluşturulmuştur ve birbirlerinden bağımsızdır.
- Uygunluk sorumluluğu bir üst düzey yöneticiye aittir. Bir işletmenin üst yönetim perspektifinden bakıldığında, istenen performansa ulaşmak için yetki ve hesap verebilirliğin bir kişide olması daha kolay iletişim kurulacağı ve izlenebileceğinden arzulanır. Tabii ki bu, temel işletme faaliyetleri için olduğu kadar finans, teknoloji ve insan kaynakları gibi alanlar için de geçerlidir. Uygunluk sorumluluğu, şirketin genel hukuk danışmanı veya uygunluktan sorumlu yöneticisi tarafından üstlenilir ve bu kişi, kuruluşun tabi olduğu tüm yasal ve düzenleyici gereklilikleri yerine getirmesini sağlamakla görevlidir. Bu yaklaşım, böylesi merkezi bir sorumluluk atamada fayda gören yönetim kurulları tarafından da benimsenmektedir. Bazı açılardan avantajlı gibi görünse bile, gerçek şu ki, bu yaklaşım uygunluğun yerine getirilmesi için sorumluluğun yanlış yere yerleştirilmesine yol açar.
- Bir başka faktör de uygunluğu yalnızca maliyetleri yükselten bir zorunluluk olarak görmektir. Kuşkusuz bu düşünceye göre, işletmeyi büyütmek ve karlılığı artırmak için kullanılması gereken kaynaklar boşa harcanır. Bu felsefe işletmeye zarar verebilir.

### *3.4.3.4. Uygunluk fonksiyonunun temel sorumlulukları*

Uygunluk çalışanlarının rolü endüstriye ve ele alınması gereken düzenlemelerin türüne göre değişmekle birlikte, uygunluk uzmanlarının çoğu için gereken ortak bir görev tanımı bulunmaktadır. Bunlar dört ana kategoriye ayrılabilir: (1) yasa, düzenleme ve işletme politikalarını takip etme ve değerlendirme, (2) uygunluk politikaları geliştirme ve uygulama, (3) eğitim ve rehberlik, (4) izleme, denetleme ve belgelemedir. Bunlar kısaca açıklanmıştır (Peak, 2012, s. 5):

- Kuralların Tanımlanması, İzlenmesi ve Değerlendirilmesi: Uygunluk personeli hangi yönetmeliklerin yürürlükte olduğu ve işletme faaliyetleri için nasıl uygulandıklarının anlaşılmasından sorumludur.
- Politikaların Geliştirilmesi ve Uygulanması: İşletmeler uyum için gerekli olan belirli önlemlere karar vermeli ve bunları işletme çapında uygulamalıdır. Uygulama yordamları davranış kuralları, yeni usul ve kontrolleri, eğitim ve iletişimi içerebilir. Politikalar, bireylerin, süreçlerin ve ilişkilerin istendiği gibi davranış veya eylemler geliştirmesi için kurallar koyan belgelerdir. Politikalar genellikle üst düzey ve stratejiktir; içerik, hareket tarzı veya niyetleri belirler ve doğası gereği kısa olurlar. Yordamlar ise, bir politikaya uymanın formel olarak yolunu gösteren belgelerdir.
- Eğitimler ve Tavsiyeler Geliştirilmesi: Uygunluk fonksiyonu, politikalar, yordamlar, uygunluk el kitapları, iç davranış kuralları ve uygulama talimatları gibi dokümanlar yoluyla yasaların, kuralların ve standartların gerektiği gibi uygulanması konusunda çalışanlara yazılı rehberlik sunmaktan sorumludur.
- İzleme, Denetleme ve Belgelendirme: Uygunluk birimi çalışanları, politikaların ve yordamların takip edildiğinden ve uyum çabalarının açıkça belgelendirilmiş olduğundan emin olmalıdır. Bu izleme ve uygulama rolünde, disiplin kuralları, politikalara uyulmadığında olumsuz sonuçlarla karşılaşılacağına dair çalışanlara açık bir mesaj verme konusunda yeterli netlikte olmalıdır.

### *3.4.3.5. Uygunluk programı*

Geniş bir anlayışla, uygunluk, yönetişimin etkili olmasına yardımcı olan önemli bir mekanizmadır. Uygunluğun izlenmesi ve sürdürülmesi, sadece düzenleyici kesimleri memnun etmek için yapılmaz; mevzuat gerekliliklerine ve organizasyonun kendi politikalarına uygunluk, aynı zamanda etkin risk yönetiminin kritik bir bileşenidir. Bir organizasyonun amaçlarına ulaşması, etik iklimini koruması, uzun vadeli refahını

desteklemesi ve işletme değerlerini desteklemesi ve korumasının en önemli yollarından biridir. Etkili bir uygunluk programı, gereken sorumluluk ve hesap verebilirliğe sahip kişiler tarafından yönetilen iyi organize edilmiş bütünleşik süreçlerden oluşur. Uygunluk zor bir süreç olabilir, ancak aynı zamanda tüm organizasyonda operasyonel etkinliğe ulaşmak için bir fırsattır (Swanson, 2006, s. 1).

Uygunluk programı, genel olarak, yasaların ve yönetmeliklerin ihlal edilmesini önlemeye ve tespit etmeye yardımcı olmak için bir sürecin içindeki işletme politikalarını, yordamlarını ve eylemlerini belirleyen formel bir program olarak tanımlanır. Operasyonel bir program olduğundan sadece işletmenin davranış kuralları veya etik kodlarının belirlenmesinden çok daha fazlasını düzenler. Açıkçası davranış kuralları, bir uygunluk programının önemli bir bileşenidir ve etik, işletmenin uygunluk programının kalbi ve ruhudur. Bununla birlikte, kapsamlı bir program, işletmenin spesifik risklerine karşı kurallar belirlemeli ve önlemler geliştirmelidir (Kral, 2009, s. 2).

Etkili bir uygunluk programı birçok aşamadan oluşur. İlk adım, işletmeyi ve işletmenin uygunluk yükümlülüklerini belirleyen yasal ve düzenleyici gereklilikleri kapsayan işletmenin faaliyet gösterdiği çevreyi anlamaktır. Bir işletme geçmişinin, çalışanlarının, ihtiyaçlarının ve elde ettiği fırsatların bir yansımasıdır. İşletmeler; kanunlar ve yönetmeliklerin yanı sıra iç ve dış paydaş beklentileriyle de karşı karşıyadır. Etkili bir uygunluk programı bu dinamikleri anlamak ve yönetmek zorundadır (Silverman, 2008, s. 106).

Etkili bir uygunluk programının birçok yönü ve faktörü vardır. Yasal ve işletme içi düzenlemelerin ihlal edilmesini önlemek amacıyla asgari koşulları belirleyen bir uygunluk ve etik programının uygulanması danışmanlar, kar amacı gütmeyen kurumlar ve düzenlemeler getiren devlet kurumları tarafından önerilmektedir. Etkili bir uygunluk programının oluşturulmasına yönelik bazı yönler şöyle sıralanabilir. Bu liste, işletmenizin ne durumda olduğunu görmek için bir kontrol listesi olarak kullanılabilir (Kral, 2009, s. 3).

1. Kapsamı anlayın: Örgütsel sorumlulukları doğru bir şekilde düzenlemek amacıyla, tüm yasal ve iç uygunluk gereksinimlerini belirleyin. Bunu yasalar, düzenlemeler ve operasyonel ortamlar değiştikçe periyodik olarak gözden geçirin ve özellikle sonraki üç adımla birlikte ele alın.
2. İç ve dış bilgiyi toplayın: Yönetim kurulu, üst yönetim ve çalışanlardan düşüncelerini istemek suretiyle işletmenin kolektif zekasını oluşturun. Ayrıca

sektör gelişmelerini ve uygunluk programına rakiplerin tepkilerini anlamak için işletmenin dışından bilgi toplanmalıdır. Buna, riskleri tanımlamaya yardımcı olmak için yasal işlemleri araştırmak dâhildir.

3. Amaçları belirleyin: İşletme ve işletme birimleri açısından amaçları (bir amaca ulaşmak için gerçekleştirilecek eylemler) tanımlayın. Bu, periyodik olarak yapılan stratejik planlama sürecinin önemli bir parçası olmalıdır.
4. Risk değerlendirmesi yapın: Hem nitel hem de niceliksel ölçümler açısından riskleri ve olasılıkları tanımlayın. Senaryoları bir neden-sonuç görünümünden düşünün.
5. Kontrolleri düzeltin: Süreç içindeki politikalar, yordamlar ve eylemler, amaçlara en iyi şekilde ulaşmak amacıyla riskleri kontrol altında tutmak için düzenlenmelidir.
6. Anlaşılabilirliği doğrulayın: Herkes rollerini bilmelidir. Kontrol süreci sahiplerinin uygun şekilde davranması için, uygunluk programının neden ve nasıllarını anlamaları gereklidir. Kontrol sahiplerinin görüşlerini ve endişelerini ifade edebilmeleri için, ideal olarak bir geribildirim döngüsü ile kontrollerin açık bir şekilde bildirilmesi gerekir.
7. Kültürel desteği test edin: Birçok organizasyon, işlemler üzerinde gerçek bir etkisi olmayan programlar yerleştirmiştir. İşletme kültürünün ve ilgili tüm birimlerin güçlü bir uygunluk programını destekleyip desteklemediğini belirleyin. Bunu, anketler, bağımsız incelemeler ve işletme düzeyinde kontrol değerlendirmeleri ile sağlayın.
8. Uygunluğu değerlendirin: Kontrollerin etkin bir şekilde çalışmasını sağlamak için izleme programını, iç denetimi ve özel incelemeleri uygunluk programına dahil edin. Bu çaba aynı zamanda sorumlulukların ve kontrollerin en verimli biçimde ayarlanmasını sağlamaya çalışmalıdır.
9. Eğitimi ve iletişimi sağlayın: Periyodik olarak amaçlara yönelik eğitimler sunun ve uygunluk bilgilerini işletme birimleri, küresel girişimler, ortaklar, müşteriler, tedarikçiler ve diğer paydaş gruplarıyla paylaşın.
10. Sonuçları ölçün ve yönetim kuruluna raporlayın: Üst yönetim ve yönetim kurulunun uygunluk önlemleri ve gelişmelerden haberdar olmasını sağlamak için bir raporlama kanalı geliştirin. Hem iç hem de dış faaliyetler ele alınmalıdır.

Uygunluğun kapsamı bir işletmenin diğer yönlerini de etkiler. Tablo 3.5 bir işletmenin uygunluk yaklaşımı ve kapsamını belirleme girişiminde bulunurken dikkate alması gereken konuları göstermektedir. Uygunluk temelli yeteneklerin kullanılması ve

bir işletmede teknolojilerin desteklenmesi konusundaki tutarlı bir yaklaşım, aşağıdaki potansiyel faydaları sağlayabilir (Moeller, 2011, s. 27):

***Toplam sahip olma maliyetinde azalma***: Yatırımlar birçok düzenlemeden etkilenebilir. Örneğin, birçok düzenleme tarafından dayatılan belge saklama ihtiyaçları kayıt yönetim sistemine yapılan tek bir yatırım tarafından karşılanabilir.

***Esneklik***: Uygunluğun zorlayıcılarından biri, yeni düzenlemelerin getirilmesi ve mevcut yönetmeliklerin sıklıkla değiştirilmesidir. İşletme çapında uygunluk yaklaşımı yoluyla uyum girişimlerini merkezi olarak yöneten bir kuruluş, bu değişikliklere hızla adapte olabilir.

***Rekabet Avantajı***: Geniş ve tutarlı bir uygunluk yaklaşımı, bir işletmenin kendi iş süreçlerini daha iyi anlamasını ve kontrol etmesini sağlayarak, dış veya iç baskılara daha hızlı ve doğru tepki geliştirmesine olanak tanır. Ayrıca, bazı düzenlemeler, kurumsal çapta uygunluk yapısı tarafından sağlanan asgari sermaye gereksinimlerinin azaltılması yoluyla somut işletme faydaları kazandırabilir.

**Tablo 3.5.** *Uygunluk Yapısının Bileşenleri (Moeller, 2011)*

| Uygunluğun Kapsamı | Faaliyet |
|---|---|
| Strateji | İşletme stratejisini geliştirirken hangi düzenlemelerin ilgili olduğu belirlenmelidir.<br>Uygunluğun sürdürülebilirliği herhangi bir uygunluk stratejisinin ayrılmaz bir parçası olmalıdır. |
| Organizasyon | Her bir düzenlemenin spesifik gerekliliklerini karşılamak amacıyla örgütsel yapı geliştirilmelidir. |
| Süreçler | Anahtar süreçler uygulanmalı ve belgelendirilmelidir.<br>Belgelendirilmiş süreçlerin uygunluk / düzenleme şartlarını yerine getirmek için etkin bir şekilde uygulanmasını sağlamak amacıyla denetimler veya incelemeler yapılmalıdır. |
| Uygulamalar ve Veri | Uygulamalar, her bir düzenlemenin gereksinimlerini desteklemek için tasarlanmalı, uygulanmalı ve sürekli test edilmelidir.<br>Veriler her düzenlemeye uygun olarak ele alınmalı ve korunmalıdır. |
| Araçlar | Araçlar, her bir düzenlemenin ihtiyaçlarını karşılamak üzere tasarlanmalı ve mevcut olmalıdır (Örneğin, bazı düzenlemeler, kayıtların işletme için erişime açık bir konumda hazır bulunmasını gerektirebilir.) |

Etkili YRU uygunluk süreçleri, düzenleyici temelli gereksinimleri ele alarak, işletmelerin, işletme faaliyetlerini dönüştürmelerine ve iş süreçlerinde daha derin anlayış ve öngörülebilirlik kazanmalarına yardımcı olur. İş süreçlerinin dönüşümünün altında yatan yönlendiriciler bilgiyi daha iyi yönetebilme, yasa ve düzenlemelerin dayattığı

zorunluluklara uyum gösterme, işletmeye karşı açılan davalarla karşılaşma riskini azaltma, depolama maliyetini düşürme ve işletmenin hesap verebilirliğini gösterme becerisini geliştirme gibi faydalardan oluşur.

İşletmeler, yasa ve düzenlemelerin veya işletme politika ve yordamlarının dayattığı yeni ve mevcut kuralları belirlemek, bu kuralları ihlal etme riskini kontrol altına almak ve ortaya çıkabilecek herhangi bir ihlalin hızlı ve etkili bir şekilde giderilmesini sağlamak amacıyla kapsamlı bir uygunluk programı geliştirmelidir. Başarılı bir uygunluk programı, bir kuruluşta uygunluk kültürünü yaratır ve işletmenin iyi bir kurumsal vatandaş haline gelmesine ve öyle kalmasına yardımcı olur. Her işletmenin koşulları farklı olduğu için standart bir uygunluk programı yoktur. İşletmenin büyüklüğüne ve risk profiline bağlı olarak uygunluk programı sadece etkin bir ihbar sisteminin uygulanması ve ilgili çalışanlara işletme faaliyetlerinin yürütülmesinde uygun ticari uygulamaların eğitiminin verilmesi kadar basit olabilir veya aşağıdaki faaliyetleri içeren kapsamlı bir program uygulanabilir (Moeller, 2011, s. 132):

- Uygunluk çalışanlarından oluşan özel bir ekibin kurulması.
- Ticari uygulamalarda düzenli olarak uygunluk risk değerlendirmesi yapılması ve uygunluk programının gözden geçirilmesi.
- Benzersiz operasyonel, finansal ve ticari riskler ile karşılaşan farklı işletme birimleri için detaylı rehberler ve yordamlar tasarlanması.
- İşletmenin yasa ve düzenlemeler kaynaklı gerekliliklerini takip etmek için sistemler kurulması.
- Uygunluk ile ilgili personel eğitim programlarının geliştirilmesi ve gerektikçe sürdürülmesi.

#### *3.4.3.5.1 Uygunluk programının etkinliğini artıran temel unsurlar*

Bir uygunluk programının şekli ve büyüklüğü ne olursa olsun, yeterli kaynak tahsisi yapılmalı, yönetim kurulu ve üst yönetim tarafından aktif olarak desteklenmeli ve düzgün belgelendirme yapılmalıdır. Uygunluk programının etkinliğini artıran temel unsurlar şöyle sıralanabilir (Moeller, 2011, s. 134):

- Resmi bir uygunluk birimine duyulan ihtiyacın üst düzey yönetici tarafından kabul görmesi ve gereğinin taahhüt edilmesi.
- Kuruluşun geçerli yasalara, yönetmeliklere, kodlara ve örgütsel standartlara uyma konusundaki kararlılığının açık bir bildirimini içeren uygunluk politikası. Bu

politikanın, içsel veya dışsal olarak işletme için çalışanlar tarafından anlaşılması ve üzerinde çalışılması gerekir. Büyük işletmeler uygunluk politikası ifadelerine web sayfalarında yer vermektedir.

- Denetimler yoluyla tespit edilen sorunlara çözüm getirecek ve yasaların ihlal edilmediğinden emin olacak uygunluk ile ilgili operasyonel yordamların geliştirilmesi. Tipik olarak, uygunluk rehber materyalleri, bunlarla sınırlı olmamak üzere aşağıdakileri içermelidir: (1) Devam eden hukuki zorunlulukları belirleme, ticari uygulamalar için eğitim programları, ihlalleri izleme ve raporlama, disiplin politikası / kodu ve şikayet yönetimi gibi uygunluk süreçlerini desteklemek için belgelenmiş yordamlar, (2) Kurumsal tanıtım materyallerinin yanıltıcı ya da aldatıcı olmamasını sağlamak için durum tespiti yordamları, (3) Kurallara uymaya özen gösteren çalışanlar için teşvik ve ödül programları, (4) Sözleşmeler alanında uzmanlık sahibi kurum içi komiteler tarafından ticari uygulama sözleşmelerinin incelenmesi.
- Uygunluk süreçlerini sürdürmek için aktif, devam eden bir program. Uygunluk programı ve sistemleri izlenmeli, muhafaza edilmeli, iyi belgelendirilmeli ve programın etkin ve verimli olmaya devam etmesini sağlamak için çalışanlara bildirilmelidir. Uygunluk programının bakımı, uyum hatalarının proaktif olarak tespit edilmesini ve bunların ele alınmasını sağlamak için düzenli ve devam eden kurum içi uygunluk denetimi tarafından yapılmalıdır ve bağımsız uzmanlığa sahip birinin sistemin düzgün bir şekilde muhafaza edilmesini ve mevcut düzenleme gereksinimlerini karşılamak için düzenli olarak dış incelemeleri yapmasını gerektirmektedir. Buna ek olarak, ilgili düzenleyici otoritelerle irtibat sağlanmalıdır.

#### *3.4.3.5.2 Uygunluk sürecinin başlatılması*

Her ne kadar herhangi bir değişim girişiminde olduğu gibi potansiyel engeller olsa da, bu yol aslında çok açıktır. Denenmiş yaklaşımlar arasında, işletmenin mevcut durumunu inceleyen, ne durumda olmak istendiğini belirleyen ve bunun için bir eylem planı hazırlayan çok aşamalı bir ardışık süreç kullanılabilir. Diğer bir önemli konu da sınırlı kaynakları işletmenin diğer önemli girişimlerine aktarmak isteyen üst yöneticileri ikna etmektir. Bunları göz önünde bulundurarak, deneyimlerden elde edilen beş adımlı kısa bir taslak oluşturulabilir (Steinberg, 2011, s. 38).

1. Uygunsuzluk olaylarıyla ilgili riskleri ve maliyetleri kapsayacak şekilde uygunluk yönetimine ilişkin mevcut maliyetlerin kabaca bir tahminini yapın. Bunu, destek personeli ve değişim girişiminin maliyeti ile birlikte, işletme faaliyetlerine yerleştirilmiş bir süreçle ilişkilendirin. Geliştirilmiş bir programın etkinliğinin faydası ile ihlaller sonucu karşılaşılan yaptırımların maliyetini kıyaslayın. Genelde CEO'lar ve yönetim kurulları var olan uygunluk çabalarının eksikliklerini daha önceden fark etmiş olduklarından etkin ve verimli bir uygunluk süreci oluşturmak için makul tekliflere açıktırlar.
2. Ne durumda olduğunuzu değerlendirin. Uygunluk faaliyetlerinin derinlemesine anlaşılmasını sağlamak için hem yazılı hem de yazılı olmayan uygunluk politikalarının ve yordamlarının yetkilendirme ve destek faaliyetlerini de kapsayacak şekilde mevcut durumunu düşünün.
3. Arzulanan süreçleri tasarlayın. Gelecekte olunması gereken durum geliştirilmelidir. Dizayn edilen süreçler; örgütsel yapı, yönetim tarzı ve üst yönetimin arzuladığı bir temel üzerine kurulu diğer kültürel özellikler gibi faktörleri kapsayan işletme kültürünü yansıtmalıdır. Bu bağlamda uygunluk süreci, belirlenen sorumluluklar, hesap verebilirlik ve iletişim protokolleri aracılığıyla iş ve yönetim süreçlerine yerleştirilmek üzere tasarlanmalıdır. Süreç ilkesel ve risk temelli olup uygunluk biriminin desteğiyle geliştirilen yordamların detayları, organizasyonun her tarafında operasyonel sorumluluğu olan yöneticiler tarafından değerlendirilmelidir. Dış kaynak kullanılan işletmeler, üçüncü taraf ilişkileri, müşterek yönetime tabi ortaklıklar ve eylemleri şirketin sorumluluğunda olan ilişkili taraflar da dikkate alınmalıdır.
4. Raporlama, izleme ve iletişim süreçlerini geliştirin. İki yönlü iletişimle bilgi akışı sağlanır ve analiz edilen veriler üst yönetim ve yönetim kuruluna yukarı yönlü rapor vermek için kullanılır. Teknoloji desteği; risk analizi ve hesap verebilirlik iletişime olanak tanıyacak şekilde seçilmeli ve gerektiğinde iş süreçlerine uyarlanmalıdır. Uygunluk birimi, iç denetim ve diğer birimler arasında sorumlulukların açıkça belirlendiği izleme protokolleri geliştirir.
5. Yeni tasarlanan süreci tüm işletmeye veya seçilen birimlerden başlayarak uygulayın. Çalışanların neye ihtiyaç duyduğunu tam olarak anlamalarını sağlamak için değişim yönetimi teknikleriyle birlikte yeni protokollerin her birime ve genel olarak işletmeye nasıl bir fayda sağlayacağı konusunda eğitim ve öğretim kritik

önem taşır. Çalışanlar insan kaynaklarının amaç belirleme ve performans değerlendirme süreçlerine uygun olarak işe yerleştirilmelidir. Uygunluk, mevcut işletme ve yönetim süreçlerine yerleştirildiğinden, birimlerdeki yönetim yapısı içinde yeni sorumluluklar ön plana çıkar ve uygulama giderek daha fazla rayına oturur.

#### *3.4.3.6. Etkin uygunluğun unsurları*

Bazı işletmeler hem uygunluk maliyetlerini düşürmeyi hem de verimliliği arttırmayı ve iş süreçlerinde fayda elde etmeyi başardılar. Bu başarının ardında yatan faktörler şunlardır (Steinberg, 2011, s. 31-36):

##### *3.4.3.6.1. Stratejik perspektif*

İleri görüşlü yönetim ekipleri, uygunluğu maliyetli bir zorunluluk olarak görmek yerine, yeni yasalar ve yönetmeliklerin müşterilere, çalışanlara, yatırımcılara veya topluma zarar veren işletme faaliyetleri nedeniyle ortaya çıktığı gerçeğiyle başlayarak büyük resmi gördüler. Her yasal veya düzenleyici tepki; ürün güvenliği, insan kaynakları ayrımcılığı, bilgi gizliliği ve güvenliği, çevreyi koruma, satış uygulamaları ve mali raporlama gibi alanlarda performans çıtalarını yükseltir. Anlayışlı işletme liderleri, çıtaların yükseltilmesine rağmen pazarın bu yeni standartları asgari seviye olarak gördüğünü, tüketicilerin daha yüksek seviyedeki beklentilerini karşılayan ürünleri ve hizmetleri tercih ettiğini kavramışlardır. Başarılı yöneticiler bu anlayışla, işletmenin pazar payı ve kârlılığı açısından faydalar kazanır. Birçok farklı sektörden işletme, stratejik uygunluk yönetimi sayesinde rekabet avantajı yakalamıştır. Örneğin, hem perakende hem de restoran sektörlerinde sağlıklı gıda ürünleri talebinin farkına varan işletmeler, pazar paylarını arttırmıştır. Yolcu hakları sözleşmesi yapan bir havayolu şirketi, yüksek müşteri memnuniyeti derecelerini yakalamış, pazar payını arttırmış ve rakiplerinden daha fazla karlılığa ulaşmıştır. Adil ve ileriye dönük İK programlarına sahip işletmeler en iyi personeli çekiyor ve elinde tutuyor veya güvenilir ve şeffaf finansal raporlamaya sahip olanlar yatırımcılar tarafından daha düşük riskli olarak görülüyor ve böylece düşük sermaye maliyeti elde edebiliyorlar. Bu işletmeler, yasal ve düzenleyici gereksinimlerin daha iyi bir performans talebine işaret ettiğini ve minimum gereksinimleri aşarak bu zorluğun yerine getirilebildiğini kabul etmektedir.

#### *3.4.3.6.2. İş süreçlerini düzenlemek*

Yasal ve düzenleyici gerekliliklerin ve ilgili pazar beklentilerinin arkasında yatan nedenleri bilen ileri görüşlü işletmeler, uygunluk süreçlerini şirketin işletme amaçları ile uyumlu hale getirir ve var olan iş süreçlerine yerleştirir. Bu nedenle, uygunluk sorumluluğu sadece bir uyum çalışanının değil, sorumluluk alanlarında çalışan tüm yöneticileri ilgilendirir.

Tabii ki uygunluktan sorumlu yönetici (CCO) bir uygunluk programının iyi tasarlanmış olmasını sağlamak için kritik öneme sahiptir ve uygulama için yönetime gerekli desteği sağlamaktadır. Bu sorumluluk farklı unsurların birbirine bağlı bir uygunluk programı haline getirilmesini kapsar.

Önemli bir konu, eğer uygunluk var olan yordamların üzerine üst üste eklenirse, yönetsel maliyetlerin artacağıdır. Uygunluk süreçleri, yönetim sürecinin içine yerleştirilirse ve uygunluk birimi çalışanları veya iç denetçiler tarafından test bazlı izleme faaliyetleriyle desteklenirse, etkinlik ve verimlilik artar.

#### *3.4.3.6.3. Etik ve dürüstlük üzerine kurulan program*

Bir şirketin kültürü, her şeyden önce üst yönetimin ve işletme içinde her düzeyde faaliyet gösteren yöneticilerin eylemleri üzerine kuruludur. Gerçekten etkili olabilmek için, uygunluk programı dürüstlüğe ve güçlü etik değerlere dayanan bir kültüre oturtulmalıdır. Bir uygunluk programı dürüstlük olmadan geliştirilemez ve zaman içinde yapması için tasarlanmış olan eylemleri yapamaz.

Etkili bir uygunluk programının merkezinde, işletmenin faaliyet ve kültürünü etkilemek üzere tasarlanmış bir etik politika yer alır. Politikalar gündelik gerçek sorunlarla başa çıkabilmek için anlaşılabilir, kolayca erişilebilir ve yeterince kapsamlı olmalıdır. Aynı özellikler, bir işletme sahibinin değişen koşullara karşı güncel ve tutarlı olması gereken tüm politikaları için geçerlidir.

Doğru bir uygunluk programı, işletme çalışanlarının eylemlerini etkilemelidir. İşletmenin, çalışanlarının, müşterilerinin ve diğer çıkar sahiplerinin kuralların arkasındaki nedenleri anlamaları gerekir. Gerçek şu ki, bir şeyi neden yapmaları gerektiği hakkında hiçbir fikri olmayan bir çalışan, bir kontrol listesi mantalitesiyle hareket etmeye devam edecektir. Bu nedenle, eğitim programları, işe başlamadan önce değil, iş üzerinde yapılmalı ve birim yöneticileri tarafından desteklenmelidir.

Şikâyet kanalları işletmenin çıkarlarını koruyan kendine has bir araçtır. İşletme çalışanları şikâyet kanallarının dürüstlük kültürü ve etik değerler için bir temel oluşturduğunu bilmelidir. Kanalın gerçekten kullanıcı dostu olması gerekir ve bir destek personeli soruları cevaplamak ve iletişimi kolaylaştırmak için görevlendirilmelidir; böylece, herhangi bir endişeyi raporlamada herhangi bir belirsizlik yaşanmaz. Elbette ihbar edene karşı bir misilleme ihtimalinin ortadan kaldırılması uygun bir takip eylemidir.

#### *3.4.3.6.4. Risk esaslı yaklaşım*

İşletmeler, bazen çalışanlarında uygun bir anlayış geliştirmek için aslında çok mantıklı görülen sıfır toleranslı bir yaklaşımı benimserler. Küçük hataları göz ardı etmek, uygunluğun gerçekten önemli olmadığı anlamına gelebilecek kasıtsız bir mesaj gönderebilir. Bununla birlikte gerçek şu ki, bazı kurallar diğerlerinden daha önemlidir ve kaynaklar daima sınırlıdır. Buna göre, uyumsuzluğun nerede ve nasıl olabileceği, oluşma ihtimali ve ortaya çıkması durumunda işletme üzerindeki etkisi konusunda risklerin tanımlanması gerekir. Kaynaklar amaçlanan gereksinimlere göre en iyi sonuç alınacak yerlere harcanmalı ve riskler kabul edilebilir seviyelere indirilmelidir.

#### *3.4.3.6.5. Teknoloji*

Orta ve büyük ölçekli işletmeler için teknoloji kullanımı, uygunluk süreçlerinin merkezinde yer alır. Kullanıcı dostu BT, davranış kurallarının ve diğer ilgili politikaların kolayca erişilebilir olması, devam eden eğitim süreçlerinin desteklenmesi ve olası uygunsuzluklarla ilgili bilgi sağlama gibi faaliyetleri destekleyen bir araçtır. Yasa ve düzenlemeler ile dolu işletme çevresinin giderek karmaşıklaştığı ön kabulüyle, önde gelen işletmeler uygunluğu sağlamak için manuel yöntemler yerine, uygunluk faaliyetlerinin tümünü merkezileştiren ve yönetilmelerini sağlayan teknolojiyi kullanmaya başladılar. Kritik faydalar sağlayan teknoloji, uygunluk yönetimi süreçlerini ve yöntemlerini tanımlayamaz ancak bunların kurulmasına ve işletilmesine destek sağlar. Faydaları arasında şunlar sayılabilir:

- Uygunluk başarısızlıklarının nedenleri, finansal etkileri ve uygunluk riskini azaltma eylemleri hakkında doğru bilgiye ulaşılması amacıyla yönetim kurulu ve üst yönetime gerçek zamanlı veri yönetimi ve karar desteği sağlar.

- İşletme politikası gerekliliklerine dayalı görevleri oluşturmak, onaylamak, korumak, depolamak, izlemek ve otomatikleştirmek için politika yaşam döngüsü yönetimine imkan sağlar.
- Politika eğitimleri ile farkındalık yaratmayı kolaylaştırır, anket ve ilgili testlere geri bildirim sağlar.
- Çalışanların hesap verebilirliğini sağlamak için otomatik iş akışları oluşturur.
- Kontrol testleri, anketler, ve düzenlemelere ilişkin raporlama da dahil olmak üzere süreçleri ve bilgi alımını otomatikleştirir ve düzene sokar.
- Merkezi bir politika, yordam, risk ve kontrol deposu yoluyla ölçülebilirlik ve raporlamayı destekler.

#### *3.4.3.6.6. Güçlü uygunluk birimi*

İşletmenin sektörüne ve boyutuna bağlı olarak atanan personelle yarı zamanlı veya tam zamanlı çalışabilecek bir konuma sahip uygunluktan sorumlu yönetici (CCO) uygunluk yönetimi için kritik öneme sahiptir. İşletme yöneticileri, kendi operasyonel sorumluluklarıyla ilgili mevcut ve yeni yasalar ve düzenlemeler hakkında sürekli bilgi almalıdır. Hepsinin günlük işleri vardır ve uygunluk birimi, onlara kolaylıkla uygulanan bir formda ihtiyaç duyulan bilgileri sağlamadığı sürece neyin gerekli olduğunu bilmeleri beklenemez. Daha da önemlisi, uygunluk çalışanı gereksiz bir değişiklik yapmamak için yeni yasa ve düzenlemeleri mevcut yordamların kapsamı ile karşılaştırmalı ve çakışmaları dikkate almalıdır. Birçok durumda, mevcut yordamlar yeni kurallara zaten değinebilir veya ihtiyaç duyulan yerlerde yalnızca küçük değişiklikler yapabilir. Aşırı tepkilerin kıt kaynakları gereksiz yordamlar yüzünden boşa harcaması, yetersiz tepki vermek kadar olumsuzluk yaratabilir.

Uygunluk çalışanları, organizasyonun her yerinde iletişimi teşvik edebilir ve kolaylaştırabilir. İhlallerle ilgili bilgiler, uygun eylemin ve izlemenin başlatılabilmesi için düzenli yönetsel yollar veya kanallar vasıtasıyla iletilmelidir. Bilginin işletmede yukardan aşağıya ve aşağıdan yukarıya akışı sağlanmalı ve işletmede birbirinden kopuk anlayışın yerine, işletmenin her seviyede yöneticisinin ihtiyaç halinde iletişim kurabildiği bir anlayış benimsenmelidir. Bu bağlamda üst yönetim ve nihayetinde yönetim kuruluna açık, anlaşılır ve zamanında raporlama yapılması gereklidir. Soruşturmalar ve düzeltici eylemler yapabilmek için uygunsuzluk örnekleri ve altında yatan nedenler bilinmelidir. Sorunlar tamamen anlaşılmalı ve gerekli görüldüğünde özet raporlar hazırlanmalıdır.

### *3.4.3.7. Uygunluk ve iç kontrol*

YRU kısaltmasında, işletmeleri etkileyen yasa ve kurallara uyum sağlama anlamına gelen "Uygunluğu" (Compliance) yansıtan U'nun kapsamı, kontrolleri de içine alacak şekilde geniştir. Bu anlamda bu harf, işletmede uygunluğun sağlanması ve sürekli olarak izlenmesi için düzenlenen kontrolleri simgeler. Örneğin, bir fabrikanın emisyon değerlerinin izlenmesi ya da ithalat ve ihracat belgelerinin uygun şekilde düzenlenmesi için geliştirilen kontroller, bu amaca hizmet eder. Ya da yasal düzenlemelerin istediği şekilde etkili muhasebe kontrollerinin kurulması yine uygunluğun kapsamına girer (Moeller, 2011, s. 22).

Yasal mevzuat ve işletmenin kendi politikalarına uyum gereksinimlerinin giderek artması, işletmelerde yönetim sorumluluğu olarak etkili bir iç kontrol sisteminin uygulanmasını bir zorunluluk haline getirir (Namiri & Stojanovic, 2007, s. 1). İşletmeler, çeşitli yasalar ya da yönetmeliklerden etkilenen tüm olası operasyonlarını belirlemek için hukuk danışmanlarıyla işbirliği yapmalı ve uygunluk riskleri üzerinde uygun kontroller kurmalıdır. İç denetçilerin, denetim sorumluluklarının bir parçası olarak bu kontrolleri dikkate alması beklenir; ancak genellikle ihlal belirtileri olmadıkça uygunluğun sınanması için genel olarak özel yordamların tasarlanmasına çoğu zaman gerek duyulmaz (Lynford, 2015, s. 62).

Uygunluk yönetimi, bir işletmenin devlet organları, düzenleyici kurumlar, endüstri zorunlulukları ve iç politikalar tarafından dayatılan gereklilikleri karşılaması için süreçlere ve iç kontrollere sahip olmasını garanti eder. Bir örgütsel seviyede, uygunluk, yasal ve yasal olmayan mevcut gerekliliklerin belirlenmesi, uyum sağlama durumunun değerlendirilmesi, uyum sağlamak için planlanan harcamalar karşısında uyum sağlamamanın riskleri ve potansiyel maliyetlerinin tespit edilmesi şeklinde sıralanabilen yönetim süreçleri sayesinde başarılır (Anand, 2010, s. 57).

İç denetimin esas sorumluluğu da, etkin iç kontroller geliştirmektir. İç denetim ve uygunluk fonksiyonlarının desteğiyle ve yönetimin sorumluluğuyla geliştirilen ulusal ve uluslararası çok sayıda yasa ve düzenlemenin olduğu finansal yönetim, küresel ticaret, çevrenin korunması, sağlık ve güvenlik gibi alanlarda çeşitli kontroller, uygunlukla ilişkili olarak kurulur. Bu alanların her birinde, farklı dış düzenleyiciler (devlet organları, uluslararası kuruluş ve organizasyonlar gibi) sayıları giderek artan çok sayıda karmaşık yasa ve düzenlemeyi (örneğin; ulusal ve uluslararası terörün finansmanının önlenmesi, çevre ve katı atık yönetimi kanunu, dış ticaret mevzuatı gibi) dayatmaktadır. Kontrol

formları, raporlar ve lisanslarla bu düzenlemelere uygunluğun kanıtlanması gerekebilir (Broady & Roland, 2008, s. 27).

#### *3.4.3.8. Uygunluk ve iç denetim*

Uygunluk, iç denetçinin denetim sırasında, işletmenin yasalar, yönetmelikler ve kontrol standartlarına ne ölçüde bağlı olduğu konusunda bir değerlendirme yapmasını gerektiren bir konudur. Performans Standardı 2210.A3 bunu doğrulamaktadır: "İç denetçiler, operasyonların ve programların istendiği gibi uygulanıp uygulanmadığını ve sonuçların amaçlarla tutarlılığını belirlemek amacıyla operasyonları ve programları incelemelidir."

Uygunluğu incelemek ve örgütsel yapının zarar görmediğinden emin olmak, iç denetim faaliyetinin sorumlulukları arasındadır. İşletme yönetiminin görevi, faaliyetlerin işletme politika ve yordamlarına, bağlı kalınması gereken yasa, düzenleme ve anlaşmalara uygun olarak yürütülmesini sağlamaktır. İç denetim, karmaşık güncel düzenlemeler ve faaliyet stratejileri hakkında üst yönetim ve yönetim kuruluna bilgi sunmalıdır. Uygunluğu incelerken iç denetçiler, uygunsuzluğun işletme üzerinde yaratabileceği sorunlar hakkında görüş bildirmek, uygunlukla ilgili amaçları incelemek ve yönetimi tespit edilen ihlaller hakkında bilgilendirmekten sorumludur. Örgütsel yapının ihlaller, yaptırımlar ve riskler gibi potansiyel tehlikeler karşısında ayakta kalabileceği hakkında güvence verirler (Okay, 2005, s. 18).

Genel olarak iç denetimin sorumluluğu, etkin bir uygunluk programının uygulandığından, sürekli gözden geçirildiğinden ve ilgili yönetim birimlerince onaylandığından emin olmaktır. Bu sorumluluğu gerektiği gibi yerine getirmek için iç denetçiler, YRU bakış açısıyla uygunluk süreçlerinin katılımcılarının sorumluluklarını gerektiği gibi üstlendiklerinden emin olmalıdırlar. Uygunluk sürecinin başlıca katılımcıları arasında yönetim kurulu ve üst yönetim, hukuktan sorumlu yönetici, insan kaynakları ve uygunluktan sorumlu yönetici sayılabilir (Adams, 2016, s. 113).

Düzenlemelerin sürekli değişmesi veya güncellenmesi ya da aynı alanda birden fazla düzenlemenin yer alması gibi işletmeyi zorlayıcı sorunlara karşılık, birçok işletme kapsamlı uygunluk programları uygular. Bu programların amacı, işletmenin uyum sağlaması gereken yasalar ve düzenlemeler gibi bütün önemli gerekliliklerin koordine edilmesini ve bütünleştirilmesini sağlamaktır. İç denetim işletmenin uygunluk programını bütünleştirmeyi amaçlayan bir denetim yürütür. Genel olarak iç denetim; sistemin

uygunluğu, örgütsel dizayn ve hesap verebilirlik, uygunluk biriminin faaliyetleri ve uygunluğun raporlanması üzerinde incelemeler ve değerlendirmeler yapar (Jefferson Wells, 2009, s. 4).

Sağlık Sektörü Uygunluk Birliği (HCCA) ve Sağlık Sektörü İç Denetçileri Birliği (AHIA), denetim ve izleme süreçlerinin kilit yönleri hakkında rehberlik materyalleri geliştirmek, denetim ve izlemenin daha iyi tanımlanması ve açıklanması, uygunluk ve iç denetim işlevlerinin rollerini açıklığa kavuşturmak ve organizasyonların geliştirilmesi amacıyla bir ekip oluşturmuşlardır. Bu ekip tarafından uygunluk faaliyetlerinin denetimi ve izlenmesi için aşağıdaki tavsiyeler geliştirilmiştir (Ruppert, 2006, s. 1):

- Bir risk değerlendirmesi yapın ve risk düzeyini belirleyin.
- Yasa, düzenleme ve işletme politikalarını anlayın.
- Önemli konular için politikalar üretin.
- Politikalar ve yordamlar hakkında bilgi sahibi olun ve farkındalığı paylaşın.
- Yasalara, yönetmeliklere ve politikalara uygunluğu izleyin.
- En yüksek risk alanlarını denetleyin.
- Denetimde belirlenen düzenlemeler ve konular hakkında personeli eğitin.

Özellikle bankacılık, finansal hizmetler ve perakende gibi yüksek riskli sektörlerde belirlenen yordamlara uygunluğun incelenmesi açısından, düzenli testler yapılması ve yerel şubelere yapılan ziyaretlerde bulunulması denetim çalışmasının temel yöntemleridir. Yönetim bütün faaliyetler için -özellikle de merkezden uzak yerlerde yürütülen faaliyetler için- uygun finansal yönetim standartları ve operasyonel yordamlar geliştirmelidir. Ayrıca, bu standartların uygulanma derecesini de kontrol etmelidir. İç denetim, yönetimin merkezi olmayan operasyonlar üzerinde kontrol sistemlerinin bir parçası olarak şube ziyaretleri yapmasını tavsiye eder. İç denetim biriminin işletmedeki rolünün bir parçası olarak, uygunluk kontrolleri geliştirmesi gerekebilir. Bunun için gerekli yetkilendirme ve bütçe şartları belirlenmeli ve yönetimle mutabakat sağlanmalıdır. Bu denetimler, denetçi tarafından önceden iyi programlanmış ve üzerinde yönetimle mutabakat sağlanmış ziyaretler aracılığıyla yapılmalıdır. Ancak bunların uygulanmakta olan denetim programı ile uyumlaştırılması gerekir. Ayrıca bu incelemeler, çalışma kâğıtlarında yer almalıdır. Bu tür denetimleri gerçekleştirmek için aşağıdaki yordamlar uygulanabilir (Pickett, 2010, s. 638):

1. Üst yönetimle mutabakata varılmalıdır ve bunun için planlanmış görüşmeler yapılması gerekebilir.

2. Uygun seviye yöneticilerle iletişim kurulmalı ve ziyaret için bir tarih belirlenmelidir. Ziyaret öncesinde bilgi verici bir denetim broşürü dağıtılabilir.
3. Programlanmış denetim işinde standartlaştırılmış belgeleri uygulamak mümkündür. Denetim ziyaretlerinin kaynakları aşırı tüketmesine izin verilmemeli, mümkün olduğunca genç denetim çalışanları görevlendirilmeli ve özellikle başlangıç döneminde bütçeler aşılmamalıdır. Tabi bunlar, denetimin türüne göre değişir.
4. Uzak şubeler veya operasyonlara yapılan ziyaretler; nakit işlemlerinin incelenmesi, bankacılık yasaları ve düzenlemelerini kapsayan bir işlem örnekleminin doğrulanması, tüm değerli ve taşınabilir eşyaları kapsayan envanter kontrollerinin yapılması, yerel satın alma işlemlerinin bir örnekleminin ve uygunluğunun test edilmesi, satın alma işlemlerinin maliyet merkezleri üzerindeki etkisinin incelenmesi, uygunsuzluk ve dolandırıcılığa karşı tüm zayıf alanlara bir test programının uygulanması, merkez ofise yapılan iadelerin bir örnekleminin doğrulanması, yönetimle mutabakata varılan diğer incelemelerin ve testlerin yapılması gibi denetim faaliyetlerinden oluşur.
5. Yapılan iş, denetim yönetmeliğinde belirtilen standartları karşılamalıdır ve uygun belgelendirme ve rapor formatı, denetim yöneticisinin onayına sunulmalıdır.
6. İnceleme standartları denetim yönetmeliğine uygun olmalıdır. Denetim yönetimi tarafından incelemenin izlenmesi ve performans değerlendirme belgeleri kullanılmalıdır.

Yönetim, denetim sırasında süreçler, yordamlar ve raporlar geliştirmemelidir. Bunun yerine, denetim ekibinin kuruluşun ihtiyaçlarını karşılamak için uygunluk programının çabalarını değerlendirmesini beklemelidir. Yönetim iç denetimden önce öz değerlendirme sürecini tamamlamalı ve uygunluk programının denetimi için OCEG YRU rehberi ya da başka çerçeveleri incelemelidir (Pickett, 2010, s. 642).

Yönetim, yalnızca kaynakları kontrol altında tutmak için uygun yordamları oluşturmakla kalmaz aynı zamanda bu yordamlara uyulmasını sağlamakla da yükümlüdür. İç denetim danışmanlık rolünün bir parçası olarak, yönetim adına uygunluk denetimlerini yapar ve uygun kontrolleri geliştirir. Uygunluk denetimlerini bir işletme standardı haline getiren birçok işletme vardır. Uygunluk temelli bir denetim çalışması için şu ek noktalar göz önünde bulundurulmalıdır (Pickett, 2010, s. 639):

1. Denetlenecek konular; sağlık ve güvenlik, veri koruma, güvenlik düzenlemeleri, finansal düzenlemeler, operasyonel yordamlar, bütçe kontrolü, çalışanların korunması ve fırsat eşitliği sunulması ve üst düzey politika raporlarına kadar çok farklı alanlarda olabilir. Denetçinin, uygunluk gereklilikleri ve temel mevzuat hakkında net bir kavrayışa sahip olması gerekir.
2. Uygunluk yükümlülüğünden en çok etkilenen alanlar belirlenmeli ve listelenmelidir.
3. Yönetimin uygunluk testleri ve kontrolleri yeterlilik ve etkinlik açısından soruşturulmalı ve değerlendirilmelidir.
4. Bir test programı üzerinde denetim yöneticisi ve denetimin müşterisi tarafından mutabakata varılmalıdır.
5. Test programı, denetim yönetmeliğinde belirtilen mesleki standartlara uygun olmalıdır.
6. Uygunluk testleri raporlama ve inceleme standartlarına uygun olmalıdır.

İç denetçiler uygunluk programının denetimini planlarken riske dayalı bir yaklaşım benimsemelidir. Sınırlı kaynaklara sahip denetçilerin, yalnızca yüksek riskli alanlara odaklanmaktan başka şansları yoktur ve her zaman kuruluşa en fazla değeri katmaya çalışmalıdırlar. En iyi denetim pratikleri, iç denetçilerin yalnızca uygulama sonrası program değerlendirmelerinde bulunmasını değil, uygunluk programının yaşam döngüsü boyunca denetimi yürütmelerini önerir. Uygunluk programının iç denetimi, daha genel bir denetim planının parçası olmalıdır. İç denetçiler yönetim kurulunun ve üst yönetimin uzun vadeli güvence gereksinimlerini karşılayan bir plan hazırlamalıdır (Pickett, 2010, s. 641).

İç denetimin amaçlarının tanımlanması, yönetim kuruluna ve üst yönetime sağlayacağı güvence seviyesini tanımladığı için, denetimin yönünün belirlenmesinde ilk ve en önemli adımdır. Baştan itibaren iç denetim çalışanları, denetimin işletmenin güvence ihtiyaçlarını karşıladığından emin olmak için, güvence ihtiyaçları konusunda kilit paydaşlar olan üst yönetim ve yönetim kurulu (veya gerektiğinde denetim komitesi ve hukuk danışmanı) ile görüşmelidir ve bu görüşmeler denetim planını tamamlamadan önce yapılmalıdır. Uygunluk programları çok geniş bir faaliyet yelpazesini kapsar, bu yüzden planlama aşamasının denetim çabalarının odak noktası olduğundan emin olunmalıdır. Denetim kapsamlı bir denetim risk değerlendirmesi temelinde olmalıdır, yani, iç denetçiler şirket uygunluk programının kilit risklerinin ne olduğunu

belirlemelidir. Hukuk danışmanının denetime katılımı, denetimin planlanması sırasında kararlaştırılması gereken bir başka önemli faktördür. İç denetim sırasında yanlışlık saptanırsa, hukuk danışmanıyla diyaloga ihtiyaç duyulabilir. Bu aşamada üç iç denetim amacı belirlenmelidir (Swanson, 2006, s. 2).

1. Uygunluk programının örgütsel politikalara, yürürlükteki kanunlara ve düzenlemelere uyum sağlama konusunda makul bir güvence sağlayıp sağlamadığını belirlemek;
2. Program yönetimi çerçevesinin yerinde belgelendirme yapıp yapmadığını ve işletmenin ihtiyaçlarını karşılamak için uygun kaynak tahsisi yapıp yapmadığını belirlemek;
3. Programın etkili bir şekilde uygulanıp uygulanmadığını, performans raporlama sisteminin tanımlandığı gibi program sonuçlarını doğru sunup sunmadığını belirlemektir.

İç denetçiler, denetimleri sırasında uygunluk programının başarısını etkileyen kilit faktörleri keşfetmelidir. Bu faktörler şunlardır: (1) İşletmenin farklı birimleri arasında uygunluk programlarının tutarlılığı ve bütünleştirilmesi; (2) İşletme birimleri ve uygunluk birimi arasında koordinasyon; (3) Etik, uygunluk, insan kaynakları, hukuk ve diğer ilgili birimler arasında rollerin ve sorumlulukların açık ve etkili bir şekilde düzenlenmesi.

#### *3.4.3.8.1. Uygunluk programının geliştirilmesinde risk yönetimi yaklaşımı*

Risk yönetimi ve değerlendirme, hem iç denetim hem de uygunluk için süreç döngüsünün bir parçasıdır. Risk yönetimi, olası çözümleri ve en uygun eylem biçimini seçerek riskleri gidermek için eylem ve çözümlerin tasarlanması ve uygulanması anlamına gelir. İç denetim ve uygunluk, bir organizasyonun risk yönetimi faaliyetlerinde temel bir rol oynamaktadır. Her iki meslek mensubu tarafından gerçekleştirilen birincil rol, risk değerlendirmeleri yapmaktır. Risk değerlendirme, muhtemel bir tehlikenin boyutunu belirlemek ve olumsuz sonuçların çalışanlar, işletme veya çevre için olası sonuçlarını tahmin etmek için önemli bir analitik araçtır. Risk değerlendirmeleri genellikle düzenlemeler, politikalar, süreçler, stratejiler ve organizasyonun diğer özellikleri üzerinde yürütülür (Peak, 2012, s. 6).

Risk, pek çok uygunluk biriminin gündeminde olan bir konudur. İç denetimin odak noktasında işletme genelinde yer alan her türlü risk bulunur; uygunluk birimi ise, yasa ve

düzenlemelerin uygunluk riskine odaklanır. Uygunluk birimleri yasa ve düzenlemelerin dayattığı zorunluluklardaki artış sonucunda, uyum faaliyetlerinin önceliklendirilmesini yönetmek için risk değerlendirme sürecini kullanmaktadır. Risk değerlendirme, uygunluk biriminin sınırlı kaynaklarını nerede harcayacağını, çalışanları hangi işlerde görevlendireceğini ve günlük işlemleri nasıl gerçekleştireceğini belirler. Uygunluk riski bir işletmenin kanunlara, düzenlemelere veya mevcut olan kendi düzenlemeleri veya kurallarına uymadığında yasal veya düzenleyici yaptırımlar, maddi kayıplar, itibar kaybı gibi işletme faaliyetlerinde zararla karşılaşma olasılığı olarak tanımlanabilir. Risk değerlendirme faaliyetlerinde bir potansiyel örtüşme olduğu için iç denetim ve uygunluk arasındaki planlama çabalarının eşgüdümü risk değerlendirme sonuçlarını iyileştirir ve böylece bundan hem işletme hem de her iki fonksiyon kazançlı çıkar. Risk yönetiminde bu iki birim arasında değerlendirme ve raporlama için ortak bir risk dili ve metodolojisinin kullanılması önemli katkılar sağlar (Peak, 2012, s. 7).

Uygunluk ve iç denetim için ortak metodolojiler geliştirilmesi, hangi bilgilerin nasıl toplanacağı konusunda belirsizliği giderir. Bu metodolojiler değerlendirilecek risk türlerini gözden geçirmenin kalitesini arttırır ve risk eşiklerini tanımlamak kolaylaşır. Etkili bir uygunluk programı, risklerin azaltılması veya yönetilmesi gereken eşik değerlerini, raporlama ve karar alma süreçlerinin oluşturulmasına ilişkin kuralları ve hangi kontrollerin yapılması gerektiğini tanımlayacaktır.

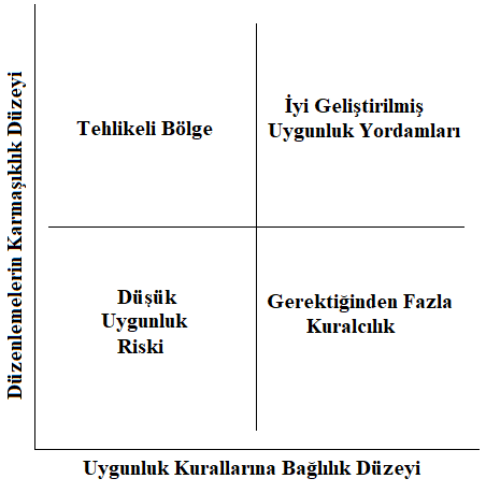
Uyumluluk konusu etkili kurumsal YRU programlarının oluşturulmasında genellikle en zor unsurdur. Bir işletme takip etmesi gereken yönetişim kurallarını kavrayan bir yönetişim çerçevesi oluşturabilir. Riskleri tahmin etmek, onlara karşı önlemler almak ve yönetmek amacıyla geliştirilen bazı iyi yordamlar oluşturulduğu için risk yönetimi, uygunluk yönetimine göre nispeten biraz daha kolaydır. Uygunlukla ilgili önemli bir sorun, çoğunlukla birbirleriyle çakışan yasa ve düzenlemelerden kaynaklanan kuralların hangisinin en önemli veya daha önemli olduğunu belirlemenin zor olmasıdır. Uyum sağlanması gereken tüm kuralların anlaşılması ve uyum sağlanması için süreçler geliştirmek zordur (Moeller, 2011, s. 144).

Planlanan iç denetimler ve geliştirilen denetim programları, muhasebe kurallarının doğru uygulanması gibi önemli iç kontrol endişelerini inceleme ve değerlendirme eğilimindedir. Sorun şu ki uygunlukla ilgili kurallara sahip pek çok kanun vardır ve geçerli kurallardan bazılarında tam bir uyum seviyesini korumak bile çok zordur. İç denetim bir çalışma birimini incelerken uyum sağlanması gereken konulardan her birinde

uygunluğu gözden geçirmek için bilgi, zaman ve kaynaklara sahiptir. Bununla birlikte yaklaşım, potansiyel ihlallerinin incelenmesi planlanan çalışma biriminin önemli risk endişesi taşıdığı yasa ve düzenlemelerin listesinden faydalanmaktır (Moeller, 2011, s. 138).

Yasa ve mevzuata uygunluk ihtiyaçları hemen hemen tüm işletmeleri etkilerken, bazıları belirli sektörleri ya da sadece işletmenin tek bir birimini etkilemektedir. Uygunluk risklerinin özellikleri, işletmenin her kademesinde anlaşılmalıdır. Bir kuruluş, uygunlukla ilgili endişeleri açısından belirli bir risk düzeyini kabul edebilir. İşletme her zaman risk iştahı ve risk felsefesiyle bağlantılı olarak kanun veya düzenlemelere karşı makul bir yaklaşım benimsemelidir. Uygunluk yönetimi, işletmenin tercih ettiği risk profiline uyum sağlamalı, uygunluk seviyesini risk profiliyle eşleşen bir düzeye getirmelidir. Yönetim kurulu, CEO ve üst yönetim, uygunluk riskini yönetmek için, işletmenin karşı karşıya bulunduğu tüm ilgili risklerin niteliğini ve kapsamını anlamalıdır (Moeller, 2009, s. 144). Hukuk birimi, kilit yöneticiler ve iç denetim yönetimin riskleri anlamasına, kategorilere ayırmasına ve tüm paydaşlara iletmesine katkı sağlayabilir (Bace vd., 2006, s. 18).

Şekil 4.10, bir işletmenin kuralları ile uygunluk çerçevesi ilişkisini göstermektedir. Yatay eksen, işletmenin uygunluk kurallarına ve yönetmeliklere uyum düzeylerini gösterir; düşük bağlılık ortamından, işletmelerin tüm kurallara ciddi olarak uymaya çalıştığı kontrol ortamına kadar uygunluk düzeylerini gösterir. Dikey eksen ise, sınırlı ve basit kurallardan, bir nükleer santralde bulunabilecek çok karmaşık kurallara kadar değişebilecek uygunluk kurallarının karmaşıklığını yansıtır. Sınırlı ve basit kuralları olan sektörlerin bir örneği perakende ticaret olabilir. Fiyatlandırma, etiketleme ve diğer birçok düzenleme de dahil olmak üzere bu alanda ulusal ve yerel kurallar giderek yaygınlaşmasına rağmen, bu kurallar birçok diğer sektörle karşılaştırıldığında daha basittir. Ulusal bir perakende zincirinin bu uygunluk kurallarını yakından takip etmesi gerekirken, daha küçük bir perakende satış işletmesinin kuralları takip etmesi gerekmeyebilir. Şekil 3.14 dört parçaya ayrılmıştır; örneğin, kurallar karmaşık olduğu halde kontrol usulleri zayıf olduğunda, işletme tehlikeli bir bölgede olabilir.




**Şekil 3.14.** *İşletmenin Kurallarının Karmaşıklık Düzeyi ile Bağlılık Düzeyi İlişkisi (Moeller, 2011, s. 136)*

İşletmeler, önemli etkileri olabilecek ve uygunluk sorunu yaratabilecek risk alanlarını tanımlamalı ve uygunluk programının geliştirilmesi için tanımlanmış riskleri kullanmalıdır. Uygunlukla ilişkili faaliyetler, süreçler ve etkinlikler için geçerli olan tüm politikalar, yordamlar, kurallar ve düzenlemeler için geçerli olmak üzere, önemli riskleri belirlemek için işletmenin her düzeyinde uygunluk sorunlarının belirlenmesi gerekir. Tablo 3.6, uygunluk risk değerlendirme sürecinin aşamalarını tanımlamaktadır:

**Tablo 3.6.** *Uygunluk Riskini Değerlendirme Süreci (Moeller, 2011)*

| |
|---|
| ***Adım 1: Uygunluk Risklerini ve ne kadar Maruz Kalındığını Belirleyin***<br>İşletme biriminin amaçlarının başarıyla sonuçlanmasını etkileyebilecek tüm uygunluk risklerinin bir listesini yapın.<br>Belirlenen riskleri yürürlüğe koymak için geçerli yasaları, kuralları, yönetmelikleri, politikayı veya yordamları belirleyin. |
| ***Adım 2: Tanımlanmış Uygunluk Risklerini Ölçme***<br>Riskli olayın gerçekleşmesi halinde, işletme biriminin amaçlarına ulaşma üzerindeki etkisi (Düşük (D)-orta (O)-yüksek (Y) şeklinde).<br>Riskin gerçek olma ihtimali (Düşük-orta-yüksek şeklinde).<br>Her riski iki karakterli bir tanımlayıcıyla kodlayın, örneğin, yüksek etki ve orta olasılık için YO gibi. |
| ***Adım 3: Belirlenmiş Uyumluluk Risklerini Önceliklendirme***<br>Öncelikler, gerçek olma ihtimalinin ve işletme birimi üzerindeki etkisinin birlikte ölçülmesiyle elde edilmelidir.<br>YY ölçüm değeri olan tüm riskler, risk envanterinin en üstüne yerleştirilmelidir. Bunu takip eden sırayla YO, YD, OY, OO, OD, DY, DO ve DD grupları yerleştirilmelidir.<br>Her ölçme değeri grubunu, eşleştirilmiş eleme işlemi vasıtasıyla en az önemli olandan en önemli olana kadar sıralayın. |
| ***Adım 4: Her Ölçüm Değeri için bir Risk Değerlendirme Matrisi geliştirin.*** |
| ***Adım 5: Risk Değerlendirme Matrisini Gözden Geçirin.*** |

Risk değerlendirme, önemli her bir örgütsel veya bütçe düzeyindeki çalışma biriminin uygulanabilir politika, yordam, kural ve yönetmeliklerin tamamına yönelik tepkileri hazırlamasını gerektirir. Bu süreç, her birime şu soruları sorarak gerçekleştirilebilir: Yasalara ve yönetmeliklere veya bu iş birimindeki kurumsal ve sistemle ilgili politikalara ve yordamlara uyum konusunda algıladığınız sorunlarınız, endişeleriniz ve algılanan riskler nelerdir? Risklere ilişkin cevaplar incelendikten sonra, birim üyeleri ve işletmenin uygunluk çalışanlarından oluşan bir ekip, bu riskler üzerindeki faaliyet ve gözetim kontrollerini tanımlamalı ve daha sonra her bir riskin potansiyel etkisini, eğer gerçekleşirse, birimin amaçları üzerindeki etkisini aşağıdaki ölçütlere göre değerlendirmelidir (Moeller, 2011, s. 138):

- ***Yüksek Etki***: Eğer risk gerçekleşirse, çalışma birimi muhtemelen amaçlarına ulaşamayacak veya büyük hasar kontrollerine ihtiyaç duyulacaktır.
- ***Orta Etki***: Eğer risk gerçekleşirse, çalışma birimi ekstra çalışmalar yapmak zorunda kalacak veya faaliyetleri verimsizleşecek, ancak yine de amaçlarına ulaşacaktır.
- ***Düşük Etki***: Eğer risk gerçekleşirse, çalışma birimi bunun farkında olacak, ancak faaliyetler veya amaçların başarılması üzerinde çok az veya hiç bir etkisi olmayacaktır.

İşletme biriminin riske karşı sorumluluğu ölçüsünde dizayn edilmesinin yanında, bir çalışan (yönetici veya çalışan düzeyinde) belirli bir uygunluk riski veya risk sorununun yönetiminden sorumlu olarak görevlendirilmelidir. Uygunluğu kontrol altında tutma stratejileri geliştirilmeli ve yönetim tarafından onaylanmalıdır. İşletmenin yasalara, kurallara ve diğer yordamlara uygun olarak faaliyet göstermeye devam etmesini sağlamak amacıyla işletme birimlerinin uygunluk konularındaki sorumlulukları güçlendirilmelidir. Ayrıca işletmenin kurallara ve düzenlemelere uyulmadığı zamanlarda düzeltme eylemi süreçlerinin geliştirilmesi için işletme çapında ve iş birimleri düzeyinde uygunluk faaliyetlerini izleyen ve inceleyen süreçlere sahip olması gerekir (Moeller, 2011, s. 138).

#### *3.4.3.8.2. Uygunluk ve iç denetim arasında koordinasyon*

Uygunluk ve iç denetim birçok ortak özelliğe sahiptir. Her iki fonksiyon da, operasyonel etkinliğe odaklanmıştır. İç denetim açısından etkinlik, denetim çıktılarından finansal performansın geliştirilmesi ve iç kontrollerin güçlendirilmesi sonuçlarının elde edilip edilmemesine bağlı olarak ölçülebilir. Böyle sonuçlar işletmenin varlıklarının korunmasına destek olur. Uygunluk açısından operasyonel etkinlik, işletmenin içinde vizyon ve misyonu destekleyen etik kültürün geliştirilebilmesine bağlı olarak ölçülebilir. Düzgün işleyen bir uygunluk programı, finansal performansın gelişmesine de yardımcı olur. Her iki fonksiyon da yönetim kuruluna, yöneticilerin işletmenin çıkarlarını en iyi şekilde koruyacak biçimde çalışması konusunda güvence sağlar. Bu güvence sahtekârlık ve diğer ahlak dışı davranışlara veya iç kontrollerin bozulmasına karşı yüzde yüz garanti veremez. Bu güvence her iki fonksiyon tarafından işletmenin geliştirilmesi için sürekli olarak çaba sarf edilmesini savunan bir metodolojiyle sağlanır (Limmroth, 2012, s. 28).

Bu iki fonksiyon arasındaki faaliyetlerin etkin bir şekilde koordine edilmesini sağlamak için, iki fonksiyonun ortak bir risk ve kontrol dilinden faydalanması şarttır. Uygunluk ve iç denetim için ortak bir metodoloji, risk türleri ve risk eşiklerinin tanımlanması konusunda anlaşmaya varılmasını sağlar. Buna ek olarak, işletmeler, ortak bir teknoloji çözümü kullanarak uygunluğu ve iç denetimi yönetmelidir. Farklı teknoloji çözümleri kullanılması, organizasyonu tutarsızlıklar ve verimsizlikler ile karşı karşıya bırakır ve sonuç olarak daha yüksek maliyet riskine sokar. Standartlaştırılmış bir BT'leri, işletme faaliyetlerinin tek bir görünümünü sağlar. Ayrıca bu fonksiyonların yönetim kurulu ile ilişkileri yoluyla iç denetim ve uygunluk birimi arasında güçlü bir bağlantı noktası kurulmalıdır. Hem iç denetim hem de uygunluk direkt olarak yönetim kuruluyla ilişki kurar ve basit bir ifadeyle, her iki fonksiyonda aynı tarafa hizmet sunar (Gillis, 2013, s. 1).

İç denetim ve uygunluk ayrı birimler olsa da, birçok ortak bağlantı noktası paylaştıkları açıktır. Bu iki birim arasındaki faaliyetlerin etkin bir şekilde koordine edilmesini sağlamak için, bu güvence gruplarının ortak bir risk ve kontrol dili, ortak yöntemler ve ortak bir teknoloji yazılımından yararlanması iyi bir çözümdür. Risklerin ve kontrollerin kapsamlı bir değerlendirmesi, standart risk ve kontrol taksonomisinin kullanılmasını gerektirir. Etkili işbirliği, risklerin ve kontrollerin iç denetim ve uygunluk ekiplerinin kabul ettiği standart modellere göre sınıflandırılmasını ve raporlanmasını

gerektirir. Riskler ve kontroller için ortak bir dil kullanmanın faydaları çok kapsamlıdır ve şunları içerir (Peak, 2012, s. 8):

- İşletmenin tamamında raporlamanın geliştirilmesi,
- Tüm risklerin dikkate alındığı tutarlı risk yönetimi,
- İşletme performansının artırılması (riskler, performans boşluklarını açıklar),
- Daha iyi risk tabanlı karar alma,
- Kontrollerin standartlaştırıldığı alanlarda daha az gözetim ve denetim ihtiyacı.

Uygunluk birimi ve iç denetim değerlendirdikleri faaliyetlerden bağımsız oldukları zaman en iyi şekilde hizmet sunabilirler. Bağımsızlığı sağlamak için, uygun yönetişim, raporlama ve yetki hiyerarşisi her iki birimin başarısının anahtarıdır. Uygunluk birimi ve iç denetim işletmenin etkili bir yönetişim ve kültüre ulaşmasına yardımcı olmak üzerine en iyi uygulama seviyesine ulaşmak için aşağıdaki pratikleri yapmalıdırlar (Ruppert, 2006, s. 2):

- Genel olarak bir denetim veya uygunluk komitesi aracılığıyla, organizasyonun yönetim kuruluna rapor verin. Bu raporlama ilişkisi, her bir görevin sorumluluklarını etkili bir şekilde ele alması için gerekli yetkileri sağlar.
- Yönetim kurulunun onayladığı bir program veya yönetmeliğe göre faaliyetleri yürütün. Kurulun onayladığı bir yönetmelik, yapılan yetkilendirmeyi belgelemektedir.
- İdari olarak kuruluşun CEO'suna raporlama yapın. Bu raporlama ilişkisi, uygunluk birimi ve iç denetim faaliyetlerine tabi operasyonel alanlardan işlevsel yönetim ve kaynak tahsisinin uygunsuz şekilde etkilenmemesini sağlar.
- Yönetim kurulu başkanı aracılığıyla genellikle yönetim kurulunun onayladığı program veya yönetmelikte tanımlandığı gibi işletmenin tamamına erişim elde edin. Uygunluk ve iç denetim çalışanları, tarafsız sonuçlar elde etmek için işletmenin kayıtlarına ve personeline açık erişim hakkına sahip olmalıdır.
- Uygunluktan sorumlu bir yöneticinin olup olmadığını ve uygunluğun sağlanıp sağlanmadığını belirleyin ve ilgili taraflara iletin. Yönetim, faaliyetlerinin yürürlükteki kanunlara, kurallara ve düzenlemelere uygun olmasını sağlamaktan sorumludur. Bu gerçek, yönetim kurulu tarafından onaylanan program veya yönetmelikte belirtilmelidir.
- Yönetimin iç kontrollerden sorumlu olup olmadığını ve iç denetimin yürütülüp yürütülmediğini belirleyin ve ilgili taraflara iletin. Yönetim, örgütsel misyon ve

stratejik hedefleri karşılamak için uygun iç kontrollerin uygulanmasını sağlamaktan sorumludur. Bu gerçek, yönetim kurulu tarafından onaylanan program veya yönetmelikte belirtilmelidir.

- Soruşturma yapma yetkisine sahip olun. Pek çok durumda uygunluk ve iç denetim araştırmalar yapmak için işbirliği yapar. Soruşturmanın doğasına bağlı olarak ya birim kendi başına ya da insan kaynakları, bilgi teknolojisi, yasa ve güvenlik gibi diğer birimlerle birlikte çalışabilir.

Her iki fonksiyon da, yönetim kurulunu ve üst yönetimi işletme içinde etkili yönetişimi geliştirmek amacıyla eğitmelidir. İşletme içinde iç ve dış gerekliliklerle uyumlu davranışlar ve uygun iç kontroller geliştirilmesinden yönetim sorumludur, iki fonksiyonda bu amacın başarılması için bağımsız olarak destek hizmeti sunar. Bu bağımsızlık, her iki fonksiyonun da politika ve yordamları etkili biçimde değerlendirmesine ve kontrolleri güçlendirme veya düzenlemelere uyum sağlamaya ilişkin ihtiyaçları karşılama konusunda yönetime öneriler getirmesine olanak tanır (Limmroth, 2012, s. 28).

İç denetim ve uygunluk birimi işletme içinde farklı rollere ve gerekliliklere sahip olsalar da, YRU yaşam döngüsü içerisinde birbirleriyle bağlantılıdırlar. İç denetim ve uygunluk arasındaki güçlü bir bağlantı noktası, yönetim kuruluyla ilişkileridir. Her ikisi de yönetim kurulunu yönlendirir ve basit bir ifadeyle, ikisi de benzer bir danışmanlık hizmeti sunar. Hem iç denetim hem de uygunluk fonksiyonları, işletmeye özel riskleri değerlendirmek ve raporlamak için hesap verebilirliğe ve yönetim kuruluyla raporlama ilişkileri için gereken bağımsızlığa sahiptir. Birbirine bağlı raporlama ilişkilerinde iç denetim ve uygunluğun ortak bir risk ve kontrol dilinden faydalanmaları ve üst yönetime daha uyumlu ve koordineli bilgi akışı sağlamak için raporlarında şeffaflığı geliştirmeleri çok önemlidir (Peak, 2012, s. 5).

İki rolün kapsamı ve bunları yerine getirmesi gereken çalışanların becerileri açısından temel farklılıklar vardır. Bu farklılıkları tanımak, her iki görevin etkin ve verimli bir şekilde yürütülebilmesi için önemlidir. Bu analiz aynı zamanda her bir birimin diğerinin çalışmalarına yardımcı olabileceği alanları belirlemeye yardımcı olabilir. Böylece çoğu zaman verimsiz olarak algılanan bu iki birime tahsis edilen sınırlı kaynaklar en iyi şekilde kullanılabilir. Potansiyel işbirliği alanlarında birimlerin birlikte iyi çalışıp çalışmadığını anlamak amacıyla aşağıdaki sorular sorulabilir (Milroy, 1995, s. 226).

- Uygunluk birimi ile işbirliği uygun şekilde belgelendirilmiş mi?

- İş süreçleri uygunluk birimiyle birlikte geliştiriliyor mu?
- İki birim arasında şube / birim ziyaretleri öncesinde yeterli irtibat sağlanıyor mu?
- Ziyaretler birlikte mi yapılmaktadır yoksa gerektiğinde işler birbirlerinin yerine yapılıyor mu?
- Bilgi değiş tokuş ediliyor mu ve ekipler düzenli olarak toplanır mı?
- İç denetim uygunluk adına araştırmalar yürütüyor mu?
- Personel değişimleri yapılıyor mu?
- Uygunluk biriminin iç denetimi yapılıyor mu?
- İç denetimin görev tanımı, uygunluk sorumluluklarını içeriyor mu?

#### *3.4.3.8.3. Ayrı uygunluk birimi kurma ihtiyacı*

Uygunluk genel olarak yasalar, düzenlemeler, sektörel ve kurumsal standartlar, sözleşmeye dayalı taahhütler, kurumsal taahhütler (örneğin, sosyal sorumluluk beyanları), değerler, etik ve kurumsal politika ve yordamlarda belirlenen yükümlülükleri yerine getirme süreci olarak tanımlanır. İç denetim ile benzer şekilde, uygunluk fonksiyonu, yönetim kuruluna ve yönetişime katkıda bulunur ve örgüt içindeki diğer rollerin geliştirilmesinde kritik bir rol oynamaktadır. İşletmede uygunluk biriminin kurulması, düzenleyici kurumlar ve uygulama örgütleri tarafından şiddetle tavsiye edilmektedir. Devlet düzenlemelerinin genişlemesi ve uygulamanın daha sıkı hale gelmesi nedeniyle endüstriden bağımsız olarak uygunluk rolü giderek önem kazanmaktadır. Uygunluk rolünün merkezinde, işletmenin karşılaştığı yaptırımlar, finansal kayıplar ve itibar kaybı gibi olumsuzlukları içinde barındıran uygunluk riskinin yönetimi yer alır (Peak, 2012, s. 4).

Finansal Hizmetler Yasası (FSA) kapsamında İngiltere'deki işletmelerde, uygunluk birimi bir zorunluluktur (Milroy, 1995, s. 223). Basel Bankacılık Denetleme Komitesi raporunda uygunluk fonksiyonunun ve faaliyetlerinin bağımsız incelemeye tabi olmasını sağlamak için uygunluk ve denetimin ayrı olması gerektiği belirtilmektedir. Risk değerlendirme ve test faaliyetlerinin iki birim arasında nasıl bölündüğü konusunda net bir şekilde belgelenmiş bir anlayışın olması gerekmektedir (Gillis, 2013, s.1).

İş sorumluluklarında benzerlikler olsa da, uygunluk ve iç denetimin ayrı birimler olarak kalması konusunda güçlü argümanlar bulunmaktadır. Ayrı birimler olmasının temel argümanı bağımsızlık kavramıdır. Bu kavram, her iki güvence fonksiyonunun

etkinliğini maksimize etmek için temel sorumlulukları ve sahip oldukları diğer sorumluluklar arasında olası bir çıkar çatışması yaşayabilecekleri bir konuma yerleştirilmemeleri gerektiğini savunmaktadır. İşletme içinde resmi statüye sahip her bir görevin önceden kararlaştırılması, yönetim yetkisinin açıkça tanımlanması ve yönetim kurulunun görev ve raporlama ihtiyaçlarının açıkça belirlenmesiyle bağımsızlığa ulaşılabilir. Bu bağımsızlığın bir parçası olarak uygunluk birimi, işletmenin diğer tüm birimleri gibi iç denetim tarafından gözetim ve incelemeye tabidir (Peak, 2012, s. 8).

Sık sık külfetli ve karmaşık uygunluk sorunlarıyla karşılaşan işletmeler, tüm uygunluk konularını bütüncül bir perspektiften yönetmek için bir uygunluk birimi kurmalıdır (Bace vd., 2006, s. 18). Böyle bir birim kurmak genellikle çok fazla özel çalışan gerektirmez. Uygunluk biriminin doğrudan çalışan desteği sınırlı olsa da, üst düzey yöneticilerin toplantılara katılması ve kendi çalışanlarını uygunluk faaliyetlerini yerine getirme yönünde görevlendirmesi olmazsa olmazdır. Uygunluk faaliyetlerinin izlenmesi ve kontrolü için örgütsel bir birim kurulmasını haklı çıkaran gerekçeler şöyle sıralanabilir (Moeller, 2011, s. 134): (1) Bir işletmenin yasal zorunluluklara uymak için adımlar atması ve ihlallerin cezai veya hukuki sorumluluğuyla yüzleşmesi zorunluluğu, (2) Kanuni durum tespiti ihtiyacı, (3) Yöneticilerin kanuni yükümlülüklerine karşı makul koruma amacıyla çalışması, (4) Yönetim kurulu üyelerinin, yasal zorunluluklarla ilgili olası ihlaller de dâhil olmak üzere işletmeyle ilgili önemli olaylardan makul bir şekilde bilgilendirilmelerini garanti eden tedbirleri alma görevleri, (5) Bireysel yetkililer ve çalışanlar tarafından yapılan ihlallerin kurumsal cezai sorumluluğunun önlenmesi, (6) İhlal durumunda cezaların engellenmesi veya hafifletilmesi, (7) Pazar dürüstlüğü kurallarına uyum için çalışılması, (8) Kanuni düzenlemelerin sayısının artması.

### 3.5. YRU Yaklaşımının Sağladığı Bütünleşik Yapı

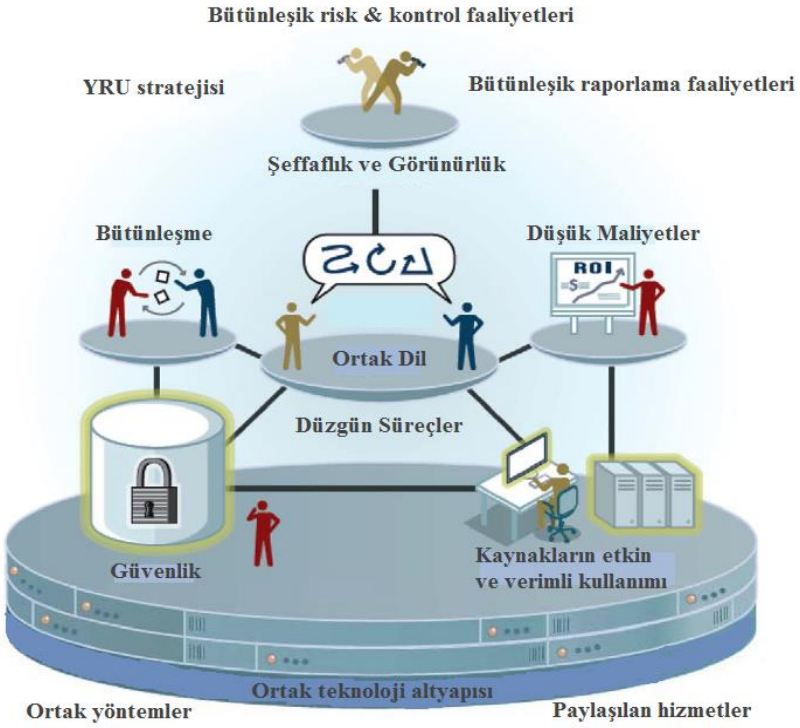
İşletme içinde birbirinden bağımsız olarak düzenlenmiş yönetişim, risk yönetimi ve uygunluk süreçleri ve birbirinden bağımsız ve iletişim halinde olmayan risk ve kontrol birimleri, bilginin işletme içinde görünürlüğünü engeller ve faydalı bilgiye ulaşılmasının önüne geçer. Bu durum, işletmede farklı birimlerde ya da süreçlerde aynı faaliyetlerin gereksiz şekilde yürütülmesine sebep olur ve bunun aksine ortak bir dil ve anlayışın oluşturulamamasına yol açar. Bu şekilde, işletme içinde birbirini gereksiz yere tekrar eden süreçler ve bu süreçlerdeki karmaşıklık artar, finansal ve beşeri kaynaklar boşa harcanır ve doğal olarak maliyetler yükselir.

Geleneksel anlayışa göre yönetişim risk ve uygunluk birbirinden kopuk bölümlerde yürütülür: Uygunluk birimi yasalar ve düzenlenmelerden kaynaklanan riskleri gidermeye çalışır; uygunluktan sorumlu yönetici (CCO) uygunlukla ilgili sorunlarla ilgilenir. Finanstan sorumlu yönetici (CFO) finansal riskle ve riskten sorumlu yönetici (CRO) bağımsız bir şekilde kurumsal risk yönetimiyle (KRY) ilgili konular hakkında çalışmalar yürütür. Sonuç olarak önemli oranda birbirini tekrarlayan çabalar ortaya çıkar. Bazı süreçler ve yordamlar birçok defa birbirinden farklı inceleyiciler tarafından kullanılan değişik standartlar ve terminolojilerle değerlendirilir. Fakat ortak bir sınıflandırma ve bütünleşik bir inceleme programını kullanan bir işletmenin, YRU gerekliliklerini yönetmek amacıyla kullandığı bütünleşik bir yaklaşım, hem YRU süreçlerindeki başarıyı hem de operasyonel etkinlik ve verimliliği en yüksek seviyeye taşır. Bütünleşik bir yaklaşımın bir diğer faydası da krizler ortaya çıkmadan önce potansiyel riskler, önemli uygunluk sorunları ve kontrolleri belirlemek amacıyla çalışan ortak proaktif süreçler geliştirerek çalışanların sahip olduğu reaktif düşünce yapısını ortadan kaldırmasıdır (Coderre, 2009, s. 96-97).

Bütünleşme kavramını şöyle bir örnekle daha iyi netleştirebiliriz. İşletmelerin eskiden birbirlerinden bağımsız çalışan envanter, faturalama, tedarik ve ücretlendirme sistemleri bulunmaktaydı. Her biri birbirinden ayrı çalışan bu sistemler genellikle mükerrer veya birbiriyle çakışan verileri işlemekte ve depolamaktaydılar. Günümüzde birçok kurum, bu faaliyetlerini bütünleştirmiştir. İlişkili veriler, kolayca toplanabilmekte ve paylaşılabilmektedir. Tedarik işlemleri, envanter verilerini güncellemektedir. Bu kökten değişimin sonucu olarak faaliyetler, stratejik olarak yönetilmeye başlamıştır. Buradan anlamamız gereken, bu faaliyetlerin birleştirilerek tek bir faaliyet olarak tek elden yönetilmesi değil, faaliyetler arasındaki bağlantıların dikkate alınması, gereksizliklere son verilmesi yani faaliyetlerin bütünleştirilmesidir.

İç politikalar, yasal düzenlemeler ve riskler gibi YRU ihtiyaçlarını daha iyi giderebilmek için, işletmede etkinliği ve verimliliği arttıran bütüncül bir bakış açısı gereklidir. Bu bakış açısına, YRU fonksiyonlarının tamamında ortak olan risk değerlendirme gibi belirli faaliyetleri ve birlikte daha iyi ve uyumlu çalışabilen risk ve kontrol fonksiyonlarını bütünleştirerek ulaşılabilir. Ayrıca bu bakış açısı bilgi, veri ve teknolojiyi daha iyi paylaşarak ve işletme içinde işbirliği kültürünü yayarak genişletilebilir. Nihai amaç, YRU alanındaki ortak süreçleri ve faaliyetleri belirlemek, bütünleştirmek ve optimize etmektir (Vicente vd., 2012, s. 1-2). İşletmenin özellikle risk

yönetimi, iç denetim, uygunluk ve iç kontrol gibi fonksiyonlarında YRU yaklaşımının sağladığı bütünleşme Şekil 3.15'te gösterilmiştir.




**Şekil 3.15.** *YRU Yaklaşımının Sağladığı Bütünleşme (OCEG, 2016)*

YRU yaklaşımının amacı işletmedeki birçok yönetişim, risk ve uygunluk sürecine sürdürülebilirlik, tutarlılık, verimlilik ve şeffaflık sağlamaktır. Bu amaca YRU ile ilgili sorumluluğu olan roller arasında işbirliği sağlanarak ve ortak bir çerçeveden ve teknoloji altyapısından faydalanılarak ulaşılabilir. Ayrıca YRU, merkezden denetlenebilen bütünleşik bir örgütsel yapıyla hareket etmeli, fakat hesap verebilirlik uygun örgütsel seviyelere dağıtılmalıdır (McClean & Rasmussen, 2007, s. 2). İşletmeler yönetişim, risk ve uygunluk süreçlerinin bütünleştirilmesine destek sağlamak için ortak bilgi, süreçler ve sistemlerden bütünleşik bir stratejiye sahip olarak faydalanabilirler. McClean & Rasmussen (2007) YRU'yu riski belirlemek, izlemek ve risk seviyesini kontrol etmek amacıyla kullanılan yeni bir yönetişim platformu olarak isimlendirmiştir. İşletme YRU stratejisine sahip olmadığında, artan riskler ve karmaşıklık karşısında daha kırılgan bir durumdadır.

Bütünleşmenin birleşme anlamına gelmediğini anlamak önemlidir. Bütünleşme daha ziyade, YRU süreçlerinde ortak bir dil, yaklaşım ve ideal teknoloji altyapısı

kullanmak anlamına gelir. Ayrıca kaynakların daha verimli bir şekilde kullanılmasını sağlar ve işletme içinde tutarlı bilgi akışını sağlayan bütün faaliyetlerin koordine edilmesi anlamına gelir. Bu şekilde, bir işletme zamanla iç denetim, muhasebe, finansal yönetim, BT güvenliği, risk yönetimi ve iç kontrol gibi fonksiyonlarının elde ettiği ilerlemeleri birbirlerine transfer edebilecektir. Bütünleşme ifadesi bir YRU sistemini kurmak için önemli birçok farklı fikri yansıtır (OCEG, 2009, s. 15-16):

1. ***YRU Disiplinlerinin Bütünleştirilmesi***: Kurumsal yönetişim, risk yönetimi, uygunluk, iç kontrol, BT, iç denetim, muhasebe, finansal yönetim gibi disiplinler hala işlerini yönetmek için farklı çerçeveler kullanırlar. Fakat bu çerçevelerin birbirlerinden farklılıktan çok benzerlikleri vardır ve işletme çeşitli YRU faaliyetlerini yönetmeye olanak tanıyan ortak bir omurga kullanarak, bunları bütünleşik bir yaklaşımla kullanabilir. Böylece işletme içinde ortak bir dil ve raporlama sağlanır.
2. ***Çeşitli Risklere Maruz Kalan Farklı Faaliyetlerin Bütünleştirilmesi***: Çeşitli risk grupları (stratejik, kültürel, operasyonel, finansal ve uygunluk gibi) işletme içinde farklı disiplinleri (iş stratejisi, finans, BT, insan kaynakları, kontrol, denetim, güvenlik gibi) etkileme potansiyeline sahiptir. Bu riskler, işletme üzerindeki yükü hafifleten ve kurumsal amaçlar için birlikte hareket edilmesini sağlayan ortak bir yaklaşımın geliştirilmesiyle etkin şekilde kontrol altında tutulabilir.
3. ***YRU Faaliyetlerinin İş Süreçleriyle Bütünleştirilmesi***: YRU faaliyetleri iş süreçleriyle bütünleştirilmelidir. Ürün geliştirme ve tasarımı, bakım ve destek hizmetleri, stratejik planlama, lojistik ve diğer ortak iş süreçleri genişletilmeli ve sayısı artırılmalıdır. Risk ve kontrol fonksiyonlarının iş süreçleri üzerinde, işletmenin stratejik amaçlarına ulaşılmasını sağlayan etkin kontrollerin geliştirilmesi sürecinde sahip oldukları tutarlı risk bilgisiyle hareket etmeleri sağlanmalıdır. Böylece uygunluk, kontrol, risk yönetimi ve iç denetim gibi risk ve kontrol fonksiyonları, ortak iş süreçleri üzerinde saptanan risklere karşı birden fazla işletme birimini etkileyen daha güçlü aksiyonlar ve etkin kontrol noktaları geliştirilmesini sağlayacaktır. Ayrıca işletme birimleri, ortak iş süreçleri üzerinde birlikte çalışma kültürünü deneyimleyecek ve işlemlerinin diğer fonksiyonları nasıl etkilediğinin bilincine varacaktır. İşletmenin organizasyon şemasının tüm parçaları, harmoni içerisinde hareket edebilecek, tehdit ve fırsatların daha fazla farkında olacak ve gereken aksiyonları çok daha çabuk geliştirecektir.

YRU yaklaşımının sağladığı bütünleşme, risk ve kontrol birimlerinin yanında diğer fonksiyonların verilerine getirdiği ortak taksonomi ile birlikte işbirliği kültürünü ve bilginin tutarlılığını sağlayacaktır. Örneğin, bir işletmede maliyet muhasebesi, müşteri karlılık analizi uygulayarak farklı müşterilerin işletmeye katkısını ölçer ve böylece müşteri karlılığının bir maliyet yönetimi aracı olarak kullanılması için pazarlama yöneticilerine ve üst yönetime kararlarında destek olur. Maliyet muhasebesi, müşteri karlılık analizi için tedarik, üretim, pazarlama, lojistik gibi fonksiyonların verilerinden hareket eder. Müşteri karlılık matrisi hazırlanır ve müşteriler işletmenin karına sağladığı katkıya göre sınıflandırılır. Diğer taraftan belirli bir müşteri grubunun bulunduğu bir ülkede gümrük vergileri yükseltilebilir ya da bölgesel terör eylemleri ülke riski doğurabilir. YRU yaklaşımının sağladığı bütünleşme, maliyet muhasebesi, pazarlama, uygunluk ve risk yönetiminin birlikte hareket etmesini ve bilginin karar süreçleri için tek bir görünümünün elde edilmesini sağlayacaktır. Böyle bir durumda, örneğin işletme yönetimi o ülkede bulunan müşteri grubunun ürün fiyatına duyarlı ucuzcu müşterilerden ya da yüksek maliyetli ve düşük kar marjına sahip saldırgan müşterilerden oluştuğu bilgisiyle hareket ederek, alternatif fırsatları dikkate alacak, ülke pazarından çıkma tercihinde bulunabilecektir.

Lojistik faaliyetlerinde yöneylem araştırması yöntemleriyle karar alan bir işletme, belirli dağıtım hatlarında ülkelerin ithal politikalarını sınırlandırması, politik sebeplerle ticari anlaşmaların askıya alınması ya da ekonomik durumun kötüleşmesi gibi sebepler yüzünden pazar payının daralma tehdidini etkin risk ve uygunluk yönetimiyle değerlendirdiğinde, gelecekte taşınması gereken minimum ürün seviyesine ulaşılamayacağını önceden belirleyebilecektir. Böyle bir tehdit karşısında çoğu zaman, alternatifler arasından fırsatların ortaya çıkarılması için uygunluk, risk yönetimi, maliyet muhasebesi, lojistik ve üretim fonksiyonları; bütünleşmenin sağladığı ortak taksonomi, süreçler, teknoloji ve terminolojiyle işbirliği içinde çalışarak üst yönetime kararlarında destek olacaktır. Söz konusu tehditlerin belirlenmesi ve kontrol altında tutulması amacıyla uygun kontrol ve eylemlerin oluşturulması için iç denetim, üst yönetimin stratejik akıl ortağı olmak zorundadır.

Bütünleşmenin faydaları arasında belki de en önemlisi, işletmede bilginin tek bir görünümünün elde edilmesi ve bu şekilde ortak bir dil ve anlayışın sağlanmasıdır. Tutarlı bilgi, özellikle risk ve kontrol çalışanlarının birbirlerini daha iyi anlamasının, doğru hareket edebilmesinin ve eşgüdüm halinde çalışabilmesinin önünü açar. Karar alma

süreçlerinin girdisi olan tutarlı bilgi, doğru sonuçlara ulaşılmasının ilk şartıdır. Üst yönetim ve yönetim kurulu aşağıdaki soruların cevabını aradığında, tutarlı bilgi, cevapların herkes tarafından aynı şekilde ortaya konması adına olmazsa olmaz hale gelir (OCEG, 2009, s. 16):

- Amaçlarımıza ulaşabiliyor muyuz?
- İlişkili riskler göz önüne alındığında, amaçlarımıza nasıl ulaşabiliriz?
- Karşılaştığımız en önemli riskler hangileridir?
- Risklerle nasıl mücadele edebiliriz ve onlardan kimler sorumlu?
- İşletmemiz tanımlanan sınırlar aşılmadan işletiliyor mu?

Daha bütünleşik ve birbirine bağlı bir yaklaşımın gerekliliği çok açıktır. Bu yaklaşım, bilgi paylaşımında işbirliğinin tesis edilmesini sağlar. Bu görüş, sadece kapsamlı bir veri tabanı ya da depo oluşturmak için uğraşmayı değil; birimler arasında daha fazla ve daha iyi iletişimin sağlanmasını da savunur. Uygun bir teknoloji altyapısı, farklı örgütsel bölümler arasında iletişimin geliştirilmesi için faydalı olabilir; fakat her şeyin daha düzgün işlemesi bütüncül bir düşünce yapısına bağlıdır. YRU yaklaşımının getirdiği bütünleşik yapı, işletme içinde bilginin tutarlı bir görünümünün elde edilmesini sağlar ve birbirinden ayrı risk ve kontrol birimlerinin birbirini tekrar eden gereksiz işlemleri yüzünden kaynakların verimsiz kullanılmasını önler (Shaim vd., 2014, s. 7).

### 3.6. YRU Yaklaşımının Faydaları

YRU yaklaşımının ilk ortaya çıkış noktası, bir işletmenin iç ve dış düzenlemelerle uyumlu, yönetişim ve risk yönetimiyle koordine biçimde faaliyet göstermesidir. YRU bileşenleri; strateji, süreçler, çalışanlar ve teknoloji kaynaklarıyla birlikte ortak bir dil, çerçeve ve altyapı oluşturmak amacıyla bütünleştirildiğinde sağlayacağı temel faydalar şunlardır (Mitchell, 2007, s. 285):

1. ***Bilgi kalitesini geliştirir.*** Düzenlemelere uyum sağlama faaliyetleri yürütülürken, bilginin tek bir şeklinin elde edilmesi önemlidir. Bir işletmenin faaliyetlerini belirlenen sınırlar içinde yürütüp yürütmediğini ve amaçlarına ulaşmak için doğru yolda olup olmadığını anlamak amacıyla, doğru bilgiye sahip olmak ta en az bilginin tutarlılığı kadar önemlidir. YRU sistemleri yönetişim, risk ve uygunluğa ilişkin bilginin, çeşitli işletme seviyelerinde analiz edilmesine ve paylaşılmasına imkân sağlar ve üst düzey yöneticilerin, yönetim kurulunun ve diğer seviyelerdeki yöneticilerin ihtiyaç duydukları bilgiye erişmelerine izin verir.

2. ***Hataları azaltır.*** Eğer bir işletmede yasalara, ulusal ve uluslararası kuruluşların getirdiği düzenlemelere ve işletmenin faaliyet alanıyla ilgili diğer standartlara uyum sağlanmazsa; para cezalarıyla, işletmenin faaliyetini sınırlandıran cezalarla hatta sorumlu işletme çalışanlarının çekmesi gereken hapis cezalarıyla karşılaşılabilir. YRU sistemleri, süreçleri standartlaştırarak, sadeleştirerek ve otomasyonla yürüterek bu tür hataların ortaya çıkmasını engeller.
3. ***Maliyetleri azaltır.*** Ortak dil, ortak süreçler, ortak teknoloji ve bazı durumlarda ortak çalışanlardan yararlanmak, YRU süreçlerini yürütmek için gereken maliyetleri azaltır. Birbirinin aynısı, lüzumsuz eylemler azaltılır. İşletme kaynakları etkin ve verimli kullanılır.

Bir işletmede YRU süreçleri, YRU yaklaşımına uygun şekilde düzenlenirse ve çalışanların bu yaklaşıma ilişkin farkındalıkları artırılırsa, işletme için fırsatlar yaratılır ve değer artışı sağlanır. OCEG, YRU yaklaşımının işletmeye sağladığı kendine özgü faydalarını şöyle sıralamıştır (OCEG, 2009, s. 18):

- Gereksiz faaliyetler belirlenir, bunlar ya düzeltilir ya da ortadan kaldırılır, böylece maliyetler azalır.
- İşletmenin tamamında birimler arasında bilginin uzlaştırılması sağlanır.
- Sistemin bütüncül bir şekilde kontrol edilmesi sağlanarak hatalar azaltılır.
- Stratejik ve taktik kararlarda kullanılan risk tabanlı bilginin kalitesi artar.
- Amaçların açıkça ifade edilmesi sağlanarak, çalışanların motivasyonu artırılır.
- Örgütsel pozisyonların uygun ve tutarlı bir şekilde düzenlenmesi ve faaliyetlerin etkili gözetimi sayesinde güven gelişir. Böylece hem işletme faaliyetlerine ilişkin üst yönetime daha fazla güvence sağlanır, hem de paydaşların işletmeye olan güveni artar.
- Paydaşların beklentileri daha etkili yönetilir.
- Beklentilerin karşılanması ve amaçlara ulaşılması için daha fazla güvence sağlanır.
- Hangi faaliyetlerin kimler tarafından hangi sırayla yürütüleceği daha öncesinde açıkça tanımlanarak belirsizlik giderilir.
- Hem finansal hem de finansal olmayan kıt kaynakların daha verimli kullanılması sağlanır.
- İşletmeye getirdiği risk ve kontrol yaklaşımı sayesinde yüksek riskli faaliyetlerin etkisi daha fazla dikkate alınır.

Price Waterhouse Coopers küresel yönetici araştırması, işletme içinde etkin YRU süreçlerinin nasıl kurulacağını ve YRU yaklaşımından elde edilebilecek faydaları 1.300'den fazla büyük ölçekli işletme yöneticisi üzerinde yapılan anketlerle ortaya koymuştur. Araştırma sonuçlarına göre YRU'nun; yasal yükümlülüklere uyum sağlanması (%64), işletmenin itibarı ve marka değeri (%56), derecelendirme kuruluşlarıyla ilişkiler (%38), finansal performans (%37), işletme faaliyetlerinin yürütülmesi (%37), işletme paydaşlarıyla ilişkiler (%33), müşteri sadakati (%32), çalışanların verimliliği (%30) ve ürün/hizmet başarısı (%30) üzerinde güçlü olumlu etkiye sahip olduğu ortaya konmuştur. Elde edilen sonuçlar, YRU yaklaşımının sadece yasa ve düzenlemelere uyum sağlamaktan çok daha fazlası olarak algılandığını göstermektedir.

2010 yılında OCEG, YRU alanında çalışmalar yürüten 343 profesyonel çalışanla YRU yaklaşımı hakkında bir anket yapmıştır. Ankete göre YRU yaklaşımı işletmelere birbirinden farklı alanlarda birçok fayda sağlamaktadır. Araştırmaya göre, bu yaklaşımdan elde edilen başlıca faydalar Şekil 3.16'da yer almaktadır.


**Şekil 3.16.** *YRU Yaklaşımının Faydaları (Adams vd., 2016, s. 10)*

OCEG'in 2015 yılı YRU araştırmasına göre, araştırmaya katılanların büyük çoğunluğu, işletmelerinde YRU yaklaşımı uygulayarak elde ettikleri olumlu faydalardan memnun olduklarını belirtmişlerdir, geriye kalanlarsa birbirinden kopuk bir yapının kendilerini başarısızlığa götürdüğünü net bir şekilde ifade etmişlerdir. Araştırmaya katılanlar bütünleşik bir yaklaşımın işletmede hâkim olmaması sonucu ortaya çıkan gereksiz ve tutarsız süreçlerin, uygunluk ve risk yönetimine güvence sağlamayı ve denetimi zorlaştırdığını (%27), gereksiz şekilde maliyetleri yükselttiğini (%22), uygunluk

ve risk yönetimi için etkin kontrollerin kurulmasını engellediği (%17), herkesin üzerinde uzlaştığı doğrulanabilir veriye ulaşmayı zorlaştırdığını (%15) ifade etmişlerdir (OCEG, 2015b, s. 11). OCEG'in araştırması, YRU yaklaşımının faydaları konusunda şu sonuçlara ulaşmıştır (OCEG, 2015b, s. 25):

- Performans ve amaçlar bağlamında riskleri yönetme yeteneğini artırır.
- Değişen ihtiyaçların ve ortaya çıkan tehditlerin belirlenmesinde, risklerin ve kontrollerin yönetilmesinde ve YRU süreçlerinde işletmeye güven verir.
- Yönetim kurulu ve üst yönetim seviyesinde risk ve uygunluğun daha fazla izlenebilmesini ve bu konuda işbirliğini geliştirir.
- Değişen riskler, yasal düzenlemeler ve işletme çevresine adaptasyon için işletmeye daha fazla esneklik sağlar.
- YRU faaliyetlerinin ve süreçlerinin yönetilmesi için, beşeri ve finansal sermayenin kullanımında verimliliği artırır.

İşletmenin yönetişim, risk yönetimi ve uygunluk süreçlerini birlikte ele almasının, işletmede iç kontrolün etkinliği üzerinde olumlu katkısı olur. Örneğin işletmenin uyum sağlaması gereken kurumsal yönetişim düzenlemeleri, işletmede kurumsal yönetişimin gelişimine katkı sağlar. Aynı zamanda bu düzenlemelere uyulmaması işletmenin maruz kaldığı çeşitli risklerin uygun seviyeye indirilmesini engelleyeceği için risk yönetimiyle de ilişkilidir. Kontrollerin hem yönetişim hem risk yönetimi hem de uygunluk bakış açısıyla geliştirilmesi etkinliğini artıracaktır. YRU'nun bütüncül bakış açısı, işletme çevresindeki değişim karşısında kontrollerin daha çabuk güncellenmesini sağlayacaktır. YRU yaklaşımı; risklerin istenen seviyede tutulmasına, kaynakların verimli kullanılmasına ve faaliyetlerin verimliliğini sağlayan uygun kontrollerin geliştirilmesine destek olur.

YRU yaklaşımının sağladığı ortak dil ve anlayış, bilginin tek ve bütüncül bir görünümünün elde edilmesi, birçok sürecin risk ve kontrol birimleri tarafından birlikte yürütülmesi ve YRU yaklaşımını destekleyen ortak teknoloji altyapısı, işletme faaliyetlerine etkin kontrollerin yerleştirilmesinin önündeki engelleri kaldırır. YRU yaklaşımı bir işletme faaliyetinin etkinliğini ve verimliliğini korumak amacıyla geliştirilen bir kontrolün başta risk ve kontrol olmak üzere tüm işletme birimleri ve çalışanları tarafından aynı şekilde anlaşılmasını ve uygulanmasını sağlar. Çünkü YRU yaklaşımı işletmenin bütünü hakkında bir bakış açısı sağlar ve iç denetçiye daha etkin ve verimli kontroller geliştirmesinde destek olacaktır. Örneğin işletmede bir faaliyet

sonucunda oluşturulan belge ve kayıtlar üzerindeki erişim listesi, aynı belge ve kayıtlardan faydalanması gereken başka bir ilişkili faaliyet geliştirildiğinde ya da yeni çalışanlar işe alındığında görevlerin ayrılığını ortadan kaldırmayacak biçimde kolayca güncellenebilecektir (Tabuena, 2010, s. 3).

### 3.7. Ortak Paylaşılan Güvence Evreni

YRU uygulamanın işletme içinde tüm güvence çalışanları özellikle de iç denetçiler için en büyük faydası, ortak kullanılan bir güvence evreni yaratmasıdır. YRU tüm çalışanların kullanabileceği ortak bir evrenin oluşturulmasına ihtiyaç duyar. Bu evren işletmeyi ortak iş terimleriyle tanımlayacak olmakla beraber tüm YRU uygulayıcıları tarafından kullanılacaktır. Bir işletmedeki YRU uygulayıcıları; iç denetim, finans, maliyet muhasebesi, BT, siber güvenlik, kalite, muhasebe, uygunluk ve risk yönetimi çalışanlarından oluşur. Bu ortak evrenden iç denetçiler, BT uzmanları, risk ve uygunluk personeli ve diğer ilgili fonksiyonların çalışanları kendi iş planlarını üretmelidir. Ancak her bir çalışan diğerinin neye ve neden baktığını bilmelidir. Böylece ortak çalışma planında boşluklar ya da gereksiz tekrarların önüne geçilebilecektir (Adams vd., 2016, s. 27).

YRU uygulandığında tüm çalışanlar kendi işlerini yapabildikleri kurumsal yönetişim, risk yönetimi ve uygunluk konularının içinde bulunduğu ortak bir evreni paylaşırlar. İşletme çalışanları bu evreni sürekli günceller ve muhafaza ederler. Bu bağlamda denetim evreni, ortak çalışma evreni içerisinde gerçekleştirilen olası denetim faaliyetlerinin bir listesidir. Ortak paylaşılan evren; yasa ve düzenlemeler, iç kontrol, risk yönetimi veya kurumsal politika ve strateji gibi birçok farklı unsuru içerir. Esasen ortak paylaşılan evren, işletmenin paydaşlarına katma değer yaratmayı sürdürdüğü ve buna dair güvence sunulması için gereken tüm bilgi ve faaliyetlerden oluşur. Paylaşılan ortak güvence evreni, ortak süreçler, terminoloji ve teknoloji altyapısı ile desteklendiğinde tüm çalışanların (özellikle güvence çalışanlarının) gereksiz faaliyetler içerisine girmesi önlenir ve riskli alanların daha kolay saptanması ve bu alanlara yönelik daha sağlam kontroller geliştirilmesinin önü açılır. YRU yaklaşımı; iç denetim, risk yönetimi, iç kontrol, uygunluk ve hatta bağımsız denetim gibi güvence çalışanlarının gerekli görülen konularda beyin fırtınası yapabilmesini kolaylaştırır, birimler arasında sinerjiyi geliştirir ve belirli kararlarda konsensüse ulaşılmasına destek olur.

### 3.8. YRU Çerçeveleri

YRU çerçeveleri, işletmelerin YRU süreçlerini etkin ve birbirleriyle koordineli bir şekilde düzenlemeleri için işletme çalışanlarına yol gösterir. İşletmelerin en iyi YRU pratiklerini elde etmelerini sağlayan bir yol haritası olarak, işletmelerin vizyon ve amaçlarına uygun yetenekleri düşünmelerine, geliştirmelerine ve sürdürmelerine destek olur ve anahtar paydaşların işletme içinde performans değerlerini görmelerine yardım eder. Bu çerçeveler, işletme içindeki birimlerde değil işletmenin tamamında başarıya ulaşılması için, YRU yeteneklerinin önemini geniş bir bakış açısıyla sunar. İşletmenin genel stratejisi ve YRU amaçlarıyla tutarlı, uygun örgütsel yapı ve kültürü yansıtan işletme süreçleri ve teknolojinin düzenlenmesine rehberlik eder (Price Waterhouse Coopers, 2004, s. 11).

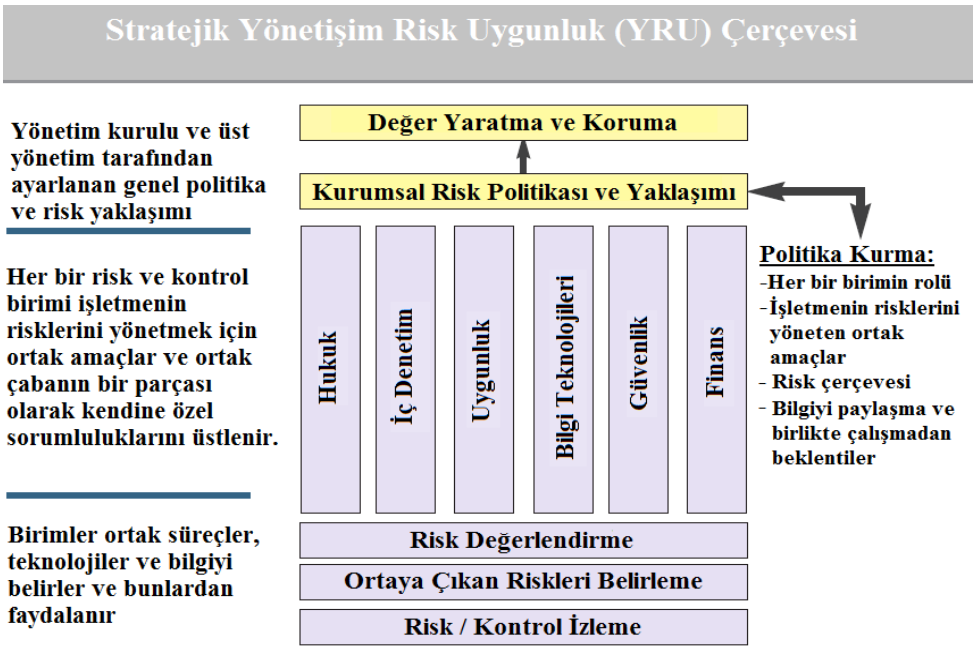
YRU işletme içinde birçok alanın birlikte ele alınmasını savunan bir disiplindir. YRU çerçeveleri de işletmenin bütününü göz önünde bulundurarak yol gösterir. Ancak YRU çerçevelerinden faydalanılması, işletme içinde belirli bir alana yönelik olarak hazırlanan başka çerçevelerin kullanılmasına veya belirli alanlarda işletmenin daha etkin ve verimli olmasına yardım etmek için hazırlanmış standartlara ve ilkelere uyulmasına engel teşkil etmez. Aksine YRU çerçeveleri bu spesifik alanlarda böyle çerçeve, standart veya ilkelere uyulmasını teşvik eder, çünkü böylece YRU yaklaşımının etkinliği de artmış olacaktır. Yönetişim alanında OECD Yönetişim İlkeleri; risk yönetimi alanında COSO Kurumsal Risk Yönetimi Çerçevesi, Basel 2 ve Solvency 2 Standartları; iç kontrol alanında COSO İç Kontrol Çerçevesi, Turnbull Kontrol Modeli, Coco Çerçevesi; bilgi teknolojileri alanında ITIL, COBIT; etik ve kurumsal sosyal sorumluluk alanında AA1000, SA8000, Küresel Raporlama Girişimi Rehberleri; kalite yönetimi alanında ISO 9000 ve altı sigma uygulanabilir (Mitchell, 2007, s. 287).

YRU yaklaşımı işletmede yönetişim, risk yönetimi ve uygunluk süreçlerini düzenleyen ve bunları bir arada değerlendiren bir yönetim disiplini olmasının yanı sıra aynı zamanda getirdiği yaklaşımın işletmede oturtulması için gereken örgütsel altyapıyı tanımlayan bir çerçevedir. Bu altyapının işletme içinde bilgi teknolojilerinin çok fazla geliştiği günümüzde işletme süreçleriyle uyumlu bilgi teknolojileri ortamıyla desteklenmesi kaçınılmazdır ve bu teknolojik yapı da YRU olarak ifade edilir. Bu durum birbirinden farklı noktaları öne çıkaran birçok YRU tanımı olmasının sebebidir. Bu bağlamda YRU'nun birbirinden farklı birçok tanımı olduğu gibi, YRU çerçevelerinin de YRU sistemlerinin ve süreçlerinin kurulması için işletmenin bütününe rehberlik sunma

amacını taşısalar da, birbirlerinden farklı bakış açıları mevcuttur. Stratejik yönetim, iç denetim, kurumsal risk yönetimi ve bilgi teknolojileri bakış açılarıyla hazırlanan birçok YRU çerçevesi vardır. Çalışmamızda iç denetimin YRU süreçlerindeki rolünü öne çıkaran ve YRU'nun sağladığı teknolojik çözümlerden daha çok, sunduğu işletme faydalarını ele alan örgütsel çerçeveler ele alınmıştır.

### 3.8.1. Stratejik yönetişim risk ve uygunluk çerçevesi

Frigo & Anderson (2009a) tarafından geliştirilen Stratejik Yönetişim, Risk ve Uygunluk Çerçevesi, işletmenin iç denetim, güvenlik, yasal uygunluk ve bilgi teknolojileri gibi birçok fonksiyonunu göz önünde bulundursa da, daha çok kurumsal risk yönetimi ve finansal uygunluk bakış açısıyla hazırlanmış bir YRU çerçevesidir. Çerçevenin temel amacı işletmenin YRU'yu daha iyi anlamasını ve işletmenin bütün birimlerinde ortak amaçların açıkça paylaşılmasını sağlamaktır. Böylece kurumsal risk yönetiminin başlıca amacı olan paydaşların korunması ve değer yaratılması sağlanır. Birimler faaliyetlerini yönetim kurulu tarafından geliştirilen işletmenin risk yönetim politikasına uygun olarak, ortak bir yönetişim şemsiyesi altında yürütür. Çerçeve her bir birimin rolünü belirler. Etkinlik ve verimlilik, ortak faaliyetler ve süreçlerden faydalanılarak artırılır. İşletme faaliyetlerinde nihai olarak değer yaratmayı amaçlayan Stratejik YRU çerçevesi Şekil 3.17'de gösterilmiştir.




**Şekil 3.17.** *Stratejik YRU Çerçevesi (Frigo & Anderson, 2009a, s. 22)*

Stratejik YRU Çerçevesi işletmenin kurumsal risk politikası ve yaklaşımını düzenler ve açıkça belirler. Bu, işletmenin stratejik risk politikalarını ve ilişkili risk yaklaşımını geliştiren yönetim kurulu seviyesindeki bir politikadır. Bu politika, işletmenin YRU birimlerinin birbirleriyle ilişkili çalışmasında ortak genel amaçları ve beklentileri düzenler. Bu ortak beklentiler şunları içerebilir (Frigo & Anderson, 2009a, s. 61):

- Bilginin paylaşılması.
- İşletme çapında bir bakış açısıyla çalışma.
- İşletme çapında bir risk çerçevesi ve dili.
- Teknolojik araçlara ortak yatırım.
- Hissedar değeri üzerindeki risklere genel bakış.

### 3.8.2. Operasyonel yönetişim risk ve uygunluk modeli

PWC, işletme içinde YRU süreçlerinde rolü olan bütün tarafların faydalanabileceği bir çerçeve olan Operasyonel Yönetişim Risk ve Uygunluk Modelini geliştirmiştir. PWC bu çerçeveyi içinde üst yöneticiler, iç denetçiler, uygunluk ve risk birimi çalışanları ve bilgi teknolojileri uzmanlarının bulunduğu anahtar YRU paydaşlarına, işletmenin vizyon ve amaçlarına uygun yetenekler geliştirmelerinde destek sunan, içinde en iyi pratiklerin olduğu bir yol haritası olarak geliştirmiştir. İşletme süreçlerinin uygun örgütsel yapı, kültür ve teknolojiyle işletmenin genel stratejisi ve amaçlarıyla tutarlı olarak uyumlaştırılmasına destek sağlar.

Operasyonel YRU Modeli işletmenin bütününü göz önünde bulunduran bir yaklaşımla, işletmenin anahtar YRU faaliyetlerini belirlemesinde, bütünleştirmesinde ve etkili yönetmesinde yol göstericidir. Kaynaklar, süreçler ve teknolojinin yönetilmesi ve stratejik şekilde konumlandırılması sayesinde, işletmenin bütünlük odaklı performansa ulaşmasına yardım etmek için tasarlanmıştır. Model, bir bütün olarak işletmenin tamamına uygulanabilir. Ayrıca işletme içindeki bir birim veya fonksiyona değer katmak için veya belirli bir alanda (belirlenen yasalara veya davranış kodlarına uyum sağlamak gibi) amaçlara ulaşmak için uyarlanabilir.

PWC YRU Modeli çalışanlar, süreçler ve teknolojilerin işletmenin vizyon ve amaçlarına uygun hale getirilmesini sağlayan dört aşamadan oluşur. Zihinde canlandırma aşaması planlama, değerlendirme ve amaçların belirlenmesi alt aşamalarından; geliştirme

aşaması harekete geçme, değiştirme ve ilerleme alt aşamalarından; işletme aşaması izleme, yürütme ve karşılık verme alt aşamalarından; sürdürme aşaması inceleme, uyum sağlama ve raporlama alt aşamalarından oluşur. Etkili YRU performansına ulaşılması ve modelin başarıyla uygulanabilmesi için aşağıda sıralanan dört anahtar değer elde edilmelidir (PWC, 2004, s. 13):

- İşletmeye doğruluk ve etik değerlerden oluşan bir kültürün aşılanması.
- İşletme süreçlerinin içine YRU yaklaşımının oturtulması.
- Performansın ölçülmesi ve elde edilen değerlerin hesaplanması.
- Teknolojiden faydalanarak etkinlik ve verimliliğe ulaşılması.

### 3.8.3. Kurumsal YRU çerçevesi

Rasmussen'in hazırladığı Kurumsal YRU Çerçevesi'nin hedef kitlesi iç denetçilerdir. Bu çerçevenin amacı, uygulama kararları ve yazılım adaptasyonunu etkileyen faktörleri belirleyerek ve tanımlayarak özellikle iç denetçilere YRU'ya ilişkin sorumluluklarını üstlenmelerinde yardımcı olmaktır. Çerçeve altı bileşenden oluşur (Rasmussen, 2009, s. 63):

- Ortak Çerçeve: İşletmedeki tüm risk ve uygunluk paydaşlarının aynı el kitabıyla hareket etmeleri gerekir. Eğer işletme içindeki farklı parçalar farklı yönlere hareket ederlerse, risk ve uygunluk faaliyetlerinde ortak anlayışın sağlayacağı sürdürülebilir ve verimli yapı için gerekli olan ekonomik faydalara ulaşılamayacaktır. Amaç, risk ve uygunluğun farklı yönlerinin işletme çapında bütünleştirilmiş bir görünümünü elde etmektir. Özel ilgi alanlarına odaklanmanın yanında, bir işletmede risk ve uygunluğun eksiksiz bir görünümünü elde etmek için ortak bir mercekle bakılabilmelidir.
- Otomatikleşme: İşletme altyapısı genişler ve hızla değişir. YRU yaklaşımında etkinliği sağlamanın tek yolu, risk ve uygunluk süreçlerini otomatikleştirmek ve işletme çevresi içinde kontrolleri güçlendirmek için işletmeye destek sunan teknolojileri uygulamaktır. Bu yaklaşım, işletme uygulamaları içinde YRU bileşenlerinin bütünleştirilmesini gerektirir. Otomasyon zaman içinde bir noktada kontrol ve değerlendirme yapmanın yanında risk ve kontrolü sürekli izlemeyi de sağlar.
- Bütünleşme: İşletmede birlikte çalışmayan teknoloji adalarından faydalanmak çok fazla zaman kaybına yol açar. Sürdürülebilir yönetişim, risk ve uygunluk süreçleri

yönetimi kolaylaştıran ve işletmenin tamamına raporlama yapan bütünleşik bir yapıdan yararlanır. Böylece risk ve uygunluk bilgisi işletmenin tamamına dağıtılır. Bu sürecin düzgün işlemesi için, esas YRU teknolojisi diğer bilgi kaynaklarıyla ve varsa diğer YRU teknolojileriyle birlikte çalışma yeteneğine sahip olmalıdır.

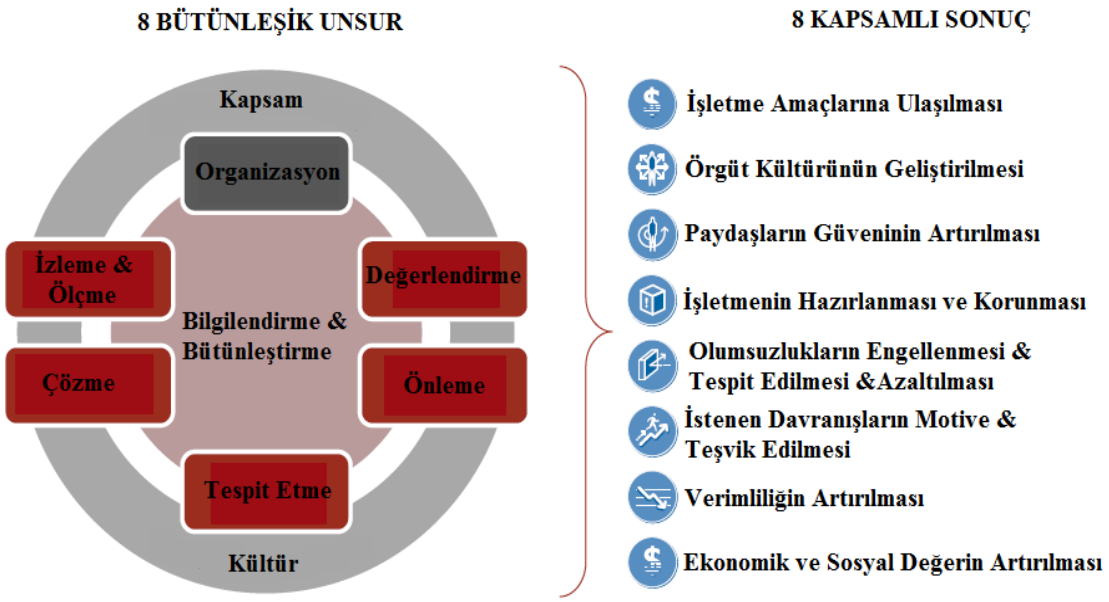
- İşletmenin tamamını kontrol etme: İşletme çevresi karmaşıktır ve yayılmıştır. İşletme süreçlerinde çalışanların, altyapının ve bilginin üzerindeki risk ve kontrollerin bütüncül bir yaklaşımla yönetilmesi gereklidir. Bilgi, uygunluk girişimlerinin ve riskin merkezidir. İşletme, bilginin kullanılabilirliği, doğruluğu ve gizliliğini belirlemek için genel bir stratejiye ihtiyaç duyar. Nihayetinde YRU yaklaşımı bütün işletme süreçleriyle ilgilidir ve işletme içinde bilginin bütüncül bir görünümünü sunamayan bir YRU teknolojisi, işletmede sorunlar yaratacaktır.
- Kullanım kolaylığı: YRU teknolojilerinin kullanıcıları bilgiye ve anlamlı bir şekilde sunulan süreç yönetimine sahip olmalıdır. İşletme kullanıcıları iş süreçlerinde kullanım kolaylığını ve verimli uygulamayı keşfetmelidir.
- Esneklik: İşletme dinamiktir ve sürekli değişim gösterir. İşletme faaliyetleri gerektiğinde değişim göstermelidir. YRU teknolojisinin iş değişikliklerine uyum sağlaması için esnek bir örgütsel ve teknolojik yapı kurulmalıdır.

### 3.8.4. OCEG YRU yetenek modeli 3.0

YRU alanında nispeten az bir zaman zarfında rehberleri ve standartlarıyla kabul gören OCEG, YRU çerçeveleri hazırlamaktadır. OCEG'in bütün dünyaya yayılmış 50.000'den fazla üyesi ve PWC, KPMG gibi denetim ve danışmanlık firmalarının da aralarında bulunduğu çok sayıda destekçisi vardır. OCEG'in esas amacı işletmelerde YRU uygulamalarını geliştirmek ve YRU'dan maksimum faydanın elde edilmesini, yani OCEG'in kendi ifadesiyle işletmelerin ilkeli performansa ulaşmalarını sağlamaktır. Bu amaç doğrultusunda OCEG, çerçevelerinin son versiyonu olan YRU Yetenek Modeli 3.0'ı 2015 yılında yayımlamıştır.

OCEG çerçevesinin amacı, bir YRU sistemini yönetmek ve uygulamaktan sorumlu olan veya bu sistemin bir bölümünde sorumlulukları olan herkes için kapsamlı bir rehber sağlamaktır. Bu rehber iç denetimden finansa, insan kaynaklarından uygunluğa, iç kontrolden bilgi teknolojilerine kadar işletme içindeki bütün alanlarda koordinasyonun sağlanması amacıyla bu alanların hepsini ayrı ayrı ele alıp, uygulayıcılara yol gösterir. 20 bileşen ve çok sayıda alt bileşenden oluşan çerçeve, işletmenin iç kontrollerinin YRU'ya

uygun olarak nasıl kurulacağından, zorunlu ve zorunlu olmayan uygunluk sınırlarının nasıl belirleneceğine kadar işletmenin yönetişim, risk ve uygunluğa ilişkin bütün alanlarını düzenler. YRU Modelinin sekiz unsuru ve modelin uygulanması sonucunda beklenen çıktılar Şekil 3.18'de verilmiştir:




**Şekil 3.18.** *YRU Modeli ve Elde Edilmesi Beklenen Sonuçlar (OCEG, 2009, s. 21)*

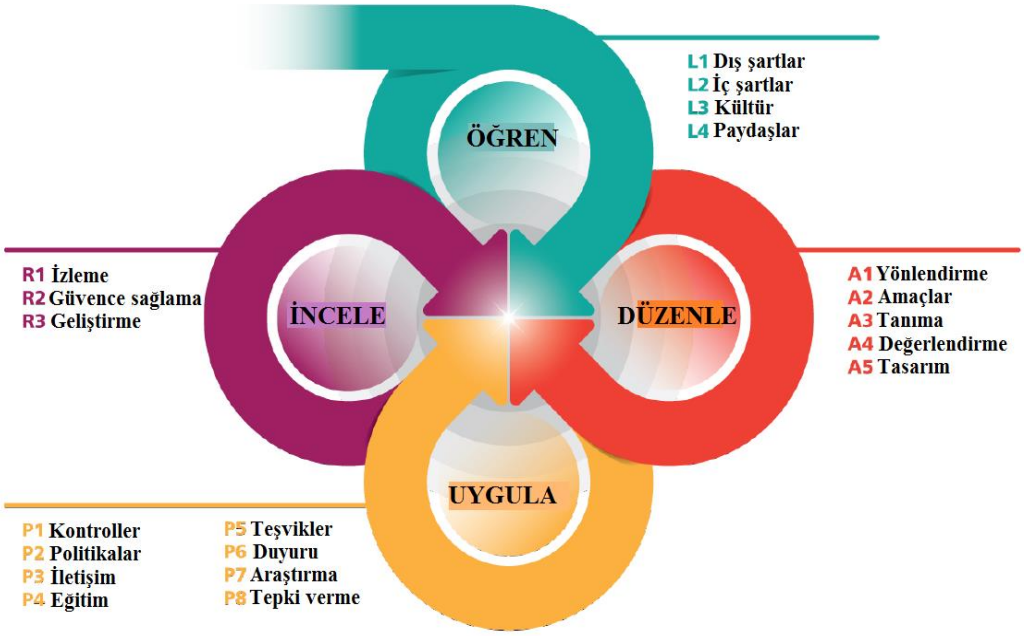
YRU Çerçevesinin sunduğu unsurlar, yönetişim, risk yönetimi ve uygunluk çabalarını örgütsel amaçları desteklemek için bütünleştirir ve üst yönetime ve çalışanlara yol gösterir. Çerçeve, işletmenin ihtiyaç duyduğu unsurları somutlaştırır. Çerçevede tanımlanan unsurlar ve ana başlıklar Tablo 3.7'de sunulmuştur (OCEG, 2009, 2015):

**Tablo 3.7.** *OCEG YRU Çerçevesi Unsurlar ve Ana Başlıklar (OCEG, 2009)*

| |
|---|
| **O. Organizasyon:** |
| O1. Bağlılık |
| O2. Roller |
| O3. Hesap Verebilirlik |
| **C. Kültür:** |
| C1. Dış İçerik |
| C2. İç İçerik |
| C3. Kültür |
| C4. Amaçlar |
| **A. Değerlendirme:** |
| A1. Risk Tanımlama |
| A2. Risk Analizi |
| A3. Planlama |
| **P. Önleme:** |
| P1. Proaktif Eylemler ve Kontroller |
| P2. Davranış Kuralları |
| P3. Politikalar |
| P4. Eğitim |
| P5. Teşvikler |
| P6. Pay Sahibi İlişkileri |
| P7. Risk Finansmanı |
| **D. Tespit Etme:** |
| D1. Bulma Eylemleri ve Kontrolleri |
| D2. Bildirim |
| D3. Sorgulama |
| **R. Çözme:** |
| R1. Tepkisel Eylemler ve Kontroller |
| R2. İç Soruşturma |
| R3. Üçüncü Taraf Soruşturma |
| R4. Krizlere Müdahale |
| R5. Kurtarma ve İyileştirme |
| R6. Getiri |
| **M. İzleme ve Ölçme:** |
| M1. İçerik İzleme |
| M2. Performans İzleme |
| M3. Sistemi Geliştirme |
| M4. Denetim ve Güvence |
| **I. Bilgi ve Bütünleşme:** |
| I1. Bilgi Yönetimi ve Belgelendirme |
| I2. İç ve Dış İletişim |
| I3. Teknoloji ve Altyapı |

OCEG Yetenek Modeli 3.0'ın bileşenleri, en temel YRU amacı olarak tanımladığı ilkeli performansa ulaşmak için sürekli olarak devam eden bir sürecin taslağını çizer. İlk etapta temel bileşenlerin bir sırası olsa da, sonrasında bileşenler aynı anda yürütülmeye başlar. Temel bileşenler aşağıda verilmiştir (OCEG, 2015a, s. 13). Şekil 3.19, OCEG YRU Yetenek Modeli 3.0'ın temel bileşenlerini göstermektedir.

- ***Öğren***: Şartları, kültürü ve paydaşları işletmenin amaçları ve stratejilerini kurmak ve desteklemek için ihtiyaç duyduğu şeyleri öğrenmek amacıyla incele ve analiz et.
- ***Düzenle***: Şartlara, kültüre ve paydaş gerekliliklerine uygun eylemleri ve kontrolleri, performansı, risk ve uygunluk amaçlarını, stratejileri, karar alma ölçütlerini düzenle.
- ***Uygula***: Proaktif, bulma ve tepki eylemleri ve kontrolleri sayesinde yapılması istenen faaliyetleri teşvik ederek ve istenmeyenleri önleyerek fırsatlar, tehditler ve ihtiyaçlara cevap ver.
- ***İncele***: Amaçlar ve stratejilerin geliştirilmesi ve düzenlenmesini de kapsayan bütün eylem ve iç kontrollerin etkili bir şekilde uygulanmasını ve tasarlanmasını geliştirmek ve izlemek için faaliyetleri yönlendir.




**Şekil 3.19.** *YRU Yetenek Modeli 3.0 (OCEG, 2015a, s. 14)*

## 3.9. YRU ve iç kontrol

YRU yaklaşımı bir işletmenin kontrol çevresinde uygulanmakta ve bu ortamı yansıtmaktadır. YRU yaklaşımı, bir işletmenin yönetim kurulu, üst yönetimi ve diğer personeli tarafından stratejik olarak ve işletme genelinde uygulanan ve işletmeyi etkileyebilecek potansiyel olayları belirlemek, bunları işletmenin risk yaklaşımına dahil etmek ve riskleri risk iştahına uygun olarak düzenlemek üzere tasarlanan, işletme amaçlarına ulaşılmasına ilişkin makul güvence sağlayan bir süreçtir. Bu bağlamda iç

kontrolü düzenleyen ve iç kontrol üzerinde yer alan bir yaklaşımdır. YRU yaklaşımının tamamen uygulandığı bir işletme çevresinde, fırsatlar ve temel riskler ile bu risklerin nasıl yönetildiği hakkında yönetime ve yönetim kuruluna zamanında bilgi sağlamak için süreçler işlemektedir. Daha da önemlisi YRU yaklaşımı sayesinde işletme çevresinde, çalışanlar rollerinin ve sorumluluklarının daha fazla farkında olmaktadırlar (PWC, 2004, s. 24). YRU çerçevesinin iç kontrolün tasarımı ve kontrollerin uygulanması konusunda getirdiği temel öneriler şunlardır (OCEG, 2015a, s. 30):

- Eylemler ve kontroller ne ihtiyaç duyulandan daha düşük bir kontrole ne de daha fazla bir kontrole yol açmalıdır.
- Eylemler ve kontroller istenen seviyedeki risk ve uygunluğu ele almalıdır.
- Gereksiz tekrarlamaların olmadığı bir dizi eylem ve kontrolle yüksek riskli alanlar için başarısızlığın önüne geçilmelidir.
- Gösterge tablolarını, uyarıları ve raporları uygun bir detay seviyesinde tanımlamak, bulma eylemleri gerçekleştiren kontrollerin anlamlı bilgiler içerdiğinden emin olmanızı sağlar.
- Eylemler ve kontroller tek bir amaçtan daha fazlasına hizmet etmelidir.
- Potansiyel olumsuz olayları ve koşulları belirlemek için geniş bir bilgi kaynakları ağı, daha fazla gözetim ve daha erken tespit sağlar.
- Sebep-sonuç ilişkilerini tanımlamak, gelecekteki uygunsuzluğu ve olumsuz davranış riskini azaltan gerekli risk ve kontrollerin düzeltilmesinde destek sağlayabilir.
- Yapılması istenen davranışların desteklenmesi, paydaşları bu tür davranışlarda bulunmaya ve istenmeyen davranışları veya şüphelenilen olayları rapor etmeye teşvik eder.
- Hem olumsuz etkilerin hem de sebeplerinin hemen düzeltilmesi gelecekteki olumsuz olay ve koşulların ortaya çıkma olasılığını azaltır.
- Eylemler ve kontroller konusunda bir sorunu çözerken ve potansiyel bir değişimi değerlendirirken, gelecekteki benzer olayların olasılığı, etkisi, zamanlaması, süresi ve sıklığı değerlendirilmesi gereken önemli hususlardır.
- Mevcut eylem ve kontrollerde yapılan değişiklikleri ve ilgili kararları belgelemek; gözetim, kararlılık ve eylem tutarlılığını göstermek için kullanılabilecek bir denetim izi ve ilgili insan kaynakları kaydı sağlar.

### 3.9.1. OCEG YRU Yetenek Modeli Modern Kontrol Sınıflandırması

YRU yaklaşımı birbirini tamamen ya da kısmen tekrarlayan kontrolleri ortadan kaldırarak, işletme ve birim düzeyindeki faaliyetler üzerinde yer alan iç kontrol maliyetlerini önemli ölçüde azaltabilir. YRU yaklaşımının sağladığı etkin iç kontrol ortamı, işletme içinde başarılı bir ortam yaratılması konusunda iç denetim için bir fırsattır. Yapılan çalışmalar, çok sayıda düzenlemeye uyum sağlaması gerekilen karmaşık bir ortamda faaliyet gösteren işletmelerde, çalışanların politika ve düzenlemelere uyum sağlamak konusunda her zaman olduğundan daha fazla baskı altında olduklarını göstermektedir. Politikalar uygun şekilde koordine edildiğinde, çalışanlar gelişmeleri için uygun bir ortam elde etmiş olacaklardır. Bununla birlikte, iç denetimin daha geniş bir kontrol yönetimine geçişi, daha fazla izleme faaliyetiyle tamamlanmalıdır. İç kontrol ortamında doğru ortak ifadeleri kullanarak değişime gitmek iç denetimin elindedir: bu süreçte iç denetim; Amaçlarımız nelerdir? Bizi amaçlara götürecek yönlendiriciler nelerdir? Mevcut süreçler optimal durumda mıdır? Sorularını sormalı ve cevapları ölçüsünde çözümler bulmalıdır (Jackson, 2007, s. 52).

Bir işletme ilkeli performansa ulaşmak için, amaçlarının peşinde koşarken belirsizliği gidermek ve dürüstlükle hareket etmek amacıyla eylemler ve kontroller uygulamalıdır. Amaçlarını destekleyen davranış ve olayları proaktif olarak teşvik etmeli ve bu amaçların gerçekleştirilmesini tehdit eden herhangi bir şeyi önlemeye çalışmalıdır. Ayrıca, amaçlar doğrultusunda süregelen ilerlemeleri tespit edebilmek ve istenmeyen davranış, koşul ve olayların oluşup oluşmadığı veya ortaya çıkma olasılığının olup olmadığı belirlenebilmelidir. Son olarak, işletme, yapılması veya ortaya çıkması istenen ve istenmeyen davranış, koşul ve olaylara uygun bir şekilde tepki vermelidir. Tepki vermek, etkili eylemler ve kontrollerin tasarlanması ve işletilmesinde hem belirlenen zayıflıkların analiz edilmesini ve değişikliklerin tavsiye edilmesini hem de pozitif davranışların desteklenmesini kapsar (OCEG, 2015a, s. 29).

Geleneksel iç kontrol modelleri, kontrolleri önleyici kontroller, bulma kontrolleri ve düzeltici kontroller olarak üç ana başlık altında sınıflandırmaktadır. Modern iş dünyasında, iç kontrole yönelik bu yaklaşımın yeterli olmadığı, geleneksel modelde ifade edilen kontrollerin kapsamının genişlediği anlaşılmıştır. Kapsamlarındaki genişleme kontrollerin yeniden ve kapsamlarını daha iyi ifade edecek yeni isimlerle sınıflandırılmasını gerekli hale getirmiştir. Bu bağlamda OCEG Modeli iç kontrolleri proaktif kontroller, bulma kontrolleri ve tepkisel kontroller olarak ifade etmiştir.

OCEG YRU Yetkinlik Modeli PERFORM bileşeninde, herhangi bir organizasyonda, amaçların karşılanmasını, riskin yönetilmesini ve uyumluluğun sağlanmasını desteklemek amacıyla ne tür eylem ve kontrollerin gerekli olduğunu incelemiştir (Switzer, Delmar & Quinlan, 2015, s. 1). YRU Yetenek Modelinde 'eylemler ve kontroller' için çok sayıda referans vardır. Bir işletme, kısa, orta ve uzun vadeli amaçları belirlerken; bunlara ulaşmak için stratejiler kurarken; performans, risk ve uygunluğu yönetmek ve güvence sağlamak amacıyla eylemler ve kontroller uygularken ele alınması gereken üç perspektifi göz önünde bulundurmalıdır. İşletmelerin proaktif, bulma ve tepkisel kontrollerin uygun bir kombinasyonunu kullanmaları gereklidir.

Kontrollerin yönetim tarafından OCEG'in sınıflandırmasına uygun şekilde ele alınması, sistemin tamamının ya da bir projenin başarıya ulaşmasının önündeki tüm aykırılıkların saptanması, engellenmesi ve düzeltilmesinin yanında başarıya ulaşılma olasılığını artıran eylemlerin yapılmasını garanti eder. İşletmenin kontrol çerçevesi, bütüncül bakış açısıyla ele alınır ve stratejiyle uyumlaştırılır. Yönetim bütüncül bakış açısıyla her kontrolün birden fazla amaca hizmet edebileceği anlayışına dayanan bir kontrol yapısı oluşturabilir. Bu durum, yüksek riskli tek bir noktaya odaklanarak bazı alanların ihmal edilmesine ya da daha fazla kontrol noktası oluşturarak aşırı kontrol karmaşasının ortaya çıkmasına engel olur. İşletme yönetimi, kontrollerin aykırılıklara karşı tepki geliştirirken aynı zamanda proaktif olabileceğinin önemini kavrar. Teknolojideki güncel gelişmelerle beraber bütüncül görünüm, kontrollerin sürekli olarak izlenmesini ve yeniden değerlendirilmesini yani sürekli kontrolü mümkün hale getirir (OCEG, 2018, s. 5).

Diğer taraftan kontrollerin kapsamını daha iyi ifade etmek amacıyla OCEG, 'eylemler ve kontroller' ifadesini kullanmaktadır. Bunun sebebi kontrol ifadesinin bazı durumlarda dar bir anlamda anlaşılmasıdır. Örneğin böyle bir kontrol anlayışına sahip bir çalışan, işletme politikalarının veya eğitim programlarının bir kontrol olmadığını, ancak politika veya eğitim programının planlandığı şekilde yapılıp yapılmadığını ölçmenin bir kontrol olduğunu savunabilir. Oysa politikalar ve eğitimler, yapılması istenen davranışları sağlamak üzere tasarlandığı için, kontroller olarak düşünülmelidir (Switzer, 2015, s. 50). OCEG'in kontrol taksonomisi Tablo 3.8'de yer almaktadır.

**Tablo 3.8.** *OCEG YRU Modeli Kontrol Sınıflandırması (OCEGa, 2015)*

| **Boyut 1** | **Boyut 2** |
|---|---|
| Proaktif Eylemler ve Kontroller | Süreç Kontrolleri |
| Bulma Eylemleri ve Kontrolleri (Detektif) | Çalışan Kontrolleri |
| Tepki Eylemleri ve Kontrolleri (Responsif) | Teknoloji Kontrolleri |
| | Finansal Kontroller |
| | Fiziksel Kontroller |

Geleneksel iç kontrol modelinde bir kontrol, temel olarak önleyici kontrollerin, bulma kontrollerinin veya düzeltici kontrollerin kapsamına girer. Aynı zamanda bu kontrolün alt boyutu olarak manuel veya teknoloji kontrollerinin, teknoloji kontrollerinin yine bir alt boyutu olarak uygulama veya genel kontrollerin kapsamına girmesi mümkündür. Örneğin müşteri hesap kodlarının işletmenin bilgi sistemine doğru girilmesi için konulmuş olan bir sağlama sayısı (check digit) kontrolü geleneksel modelde temel olarak bir önleyici kontroldür. Aynı zamanda söz konusu kontrol, alt boyut olarak sırasıyla çalışan kontrolü, BT kontrolü, uygulama kontrolü ve girdi kontrollerinin kapsamındadır. OCEG YRU Modelinde iki boyutlu bir kontrol sınıflandırması yapılmıştır. OCEG YRU Modelinin kullandığı kontrol sınıflandırmasına göre temelde üç (proaktif, bulma ve tepkisel kontroller) ana kontrol ve alt boyut olarak da beş (süreç, çalışan, teknoloji, finansal ve fiziksel kontroller) kontrol tanımlanmıştır. Böylece kontrollerin daha kolay anlaşılabilmesini ve belirlenen optimum kontrol seviyesine uygun şekilde geliştirilmesini tehdit eden karmaşıklığı ortadan kaldırmak amaçlanmıştır.

### 3.9.2. OCEG YRU Yetenek Modeli Temel Eylemler ve Kontroller

İşletmede etkin kontrollerin özellikleri ve tasarlanması, OCEG Yetenek Modeli 3.0 Çerçevesinin Uygula bölümünde 8 başlık altında ele alınmıştır. Kontroller geliştirilmeden önce, işletmenin iç ve dış şartları, kültürü ve paydaşları incelenmeli ve işletme amaçları, taktik ve stratejileri değerlendirilmelidir. Uygulama aşamasında işletmenin risk iştahına uygun kritik noktaları daha fazla dikkate alan, fırsat ve tehditlere cevap verebilmesini sağlayan, işletme faaliyetlerinin tasarlandığı gibi yürütülmesi için hataları ve hileleri engelleyen, işletme amaçlarına ulaşılması konusunda makul güvence sağlayan eylem ve kontroller geliştirilmelidir. Kontrollerin tasarlanması aşamasında YRU yaklaşımının sağladığı işletmenin bütüncül risk görünümü, ortak terminoloji ve teknolojik altyapı etkinliği ve verimliliği sağlar. OCEG kontrollerin kapsamını,

geleneksel kontrol modellerinin ötesine taşımıştır. OCEG YRU Modelinin kullandığı kontrol sınıflandırmasına göre üç temel kontrol tanımlanmıştır.

#### *3.9.2.1 Proaktif eylemler ve kontroller*

Proaktif eylemler ve kontroller önlemeyi kapsar, ancak bunun ötesine geçer. İstenen koşulları ve olayları teşvik etmek ve istenmeyen durumları önlemek için proaktif eylemler ve kontroller kullanılmalıdır. Proaktif olmak, istenmeyen davranış ve koşulları daha ortaya çıkmadan önlemek ve yapılması istenenleri belirlemek veya teşvik etmek için harekete geçmek ve eylemler/kontroller oluşturmak anlamına gelir. Proaktif olmak; performans, risk ve uygunluk koşullarını yönetmek için politikalar geliştirilmesini, eğitimler düzenlenmesini, sağlam bir iletişimin oluşturulmasını ve güçlü analizlerin yapılmasını gerektirir. Proaktif eylemler ve kontroller, istenen koşulları veya olayları proaktif olarak teşvik eder ve istenmeyenleri engeller. Proaktif kontrollerin geliştirilmesi sürecinde kilit adımlar şunlardır (Mitchell & Switzer, 2016, s. 10):

- Politikaları ve yönetim yapısını tanımlayın ve oluşturun, takip etmek için risk tabanlı yordamlar belirleyin.
- Farklı metodolojiler ve risk tabanlı eğitim müfredatları kullanan birçok iletişim kanalı ve sunma biçimi yoluyla uygun eğitim fırsatlarını tasarlayın ve sunun.
- Belirlenen bir akışta birden fazla iletişim kanalı aracılığıyla riske dayalı karar verme rehberliği ve beklentileri hakkında iletişim kurun.
- Sorunların çözülmesi için sürekli olarak operasyonel bilgileri ve temel göstergeleri izleyin
- Süreçler ve kontrolleri, risk profilleri ve iyileştirme planlarıyla uyumlu hale getirmek için gerektiği şekilde düzenleyin.

#### *3.9.2.2. Bulma (Detektif) eylemleri ve kontrolleri*

Bulma eylemleri ve kontrolleri, amaçlara yönelik ilerlemeyi belirler ve mevcut veya ortaya çıkma olasılığı olan yapılması veya ortaya çıkması istenen ve istenmeyen davranış, koşullar ve olayları tespit eder. Yapılması veya ortaya çıkması istenen ve istenmeyen davranışları ve koşulları zamanında ortaya çıkarmak, en az proaktif olarak istenildiği yönde düzenlenmeleri kadar önemlidir. Risk alma fırsatlarını keşfetmek ve aşağı yönlü riskleri belirlemek, üstün performans elde etmek için kritik önem taşır. Hem dijital hem

de insanların oluşturduğu sistemlerin iç ve dış anormallikleri ortaya çıkarması kritik derecede önemlidir. Bulma eylemleri ve kontrolleri, gerçekleşen veya gerçekleşmesi olası istenen veya istenmeyen koşullar ve olayları tespit eder. Bulma kontrollerinin geliştirilmesi sürecinde kilit adımlar şunlardır (Mitchell & Switzer, 2016, s. 10):

- Tehditler, istenmeyen davranışlar veya olaylar hakkında endişeler içeren bilgi raporlarını ve fırsatlar hakkındaki bilgiyi aktarmak için çalışanlara yollar tanımlayın.
- Tehditlerin, uygun olmayan davranışların veya koşulların erken tespiti ve olası fırsatlar için iç ve dış bilgileri toplamak amacıyla birden fazla iletişim kanalı kullanın.
- Anormallikleri, ihlalleri, uygun olmayan kontrolleri ve olası politika / yordam ihlalleri veya bunlarla ilgili erken uyarıları tespit etmek için mevcut teknoloji sistemlerini kullanın.
- Bilgileri değerlendirin, fırsatları ve sorunları çözmek için yönlendirin ve kontrolleri gerektiği gibi düzenleyin.

#### *3.9.2.3. Tepkisel (Responsif) eylemler ve kontroller*

Tepkisel eylemler ve kontroller, istenmeyen davranış, olay ve koşulları tedavi eder; belirlenen zayıflıkları düzeltir; ihtiyaç duyulan disiplini sağlar; istenen davranışları tanır ve güçlendirir; gelecekte istenmeyen davranış ve olaylar için önlem alır. Tepkisel eylemler ve kontroller hataları düzeltmekten daha fazlasını yapar. İstenmeyen davranış, olay ve koşulların düzeltilmesini sağlar; belirlenen zayıflıkları düzeltir; gerekli olan disiplini sağlar; istenen davranışları belirler ve güçlendirir ve gelecekte istenmeyen davranışları ve koşulları ortadan kaldırır. Bu kontroller, fırsatları yakalama kabiliyetimizi arttırırlar. Proaktif ve bulma kontrollerinden alınan bilginin analiz edilmesiyle eylemler yönlendirilmelidir. Olayları araştırmak ve yönetmek, fırsatları değerlendirmek veya riski yeniden değerlendirmek ve değişimi yönetmek için süreçler ve kontroller kurulduğundan emin olunmalıdır. Tepkisel kontrollerin geliştirilmesi sürecinde kilit adımlar şunlardır (Mitchell & Switzer, 2016, s. 10):

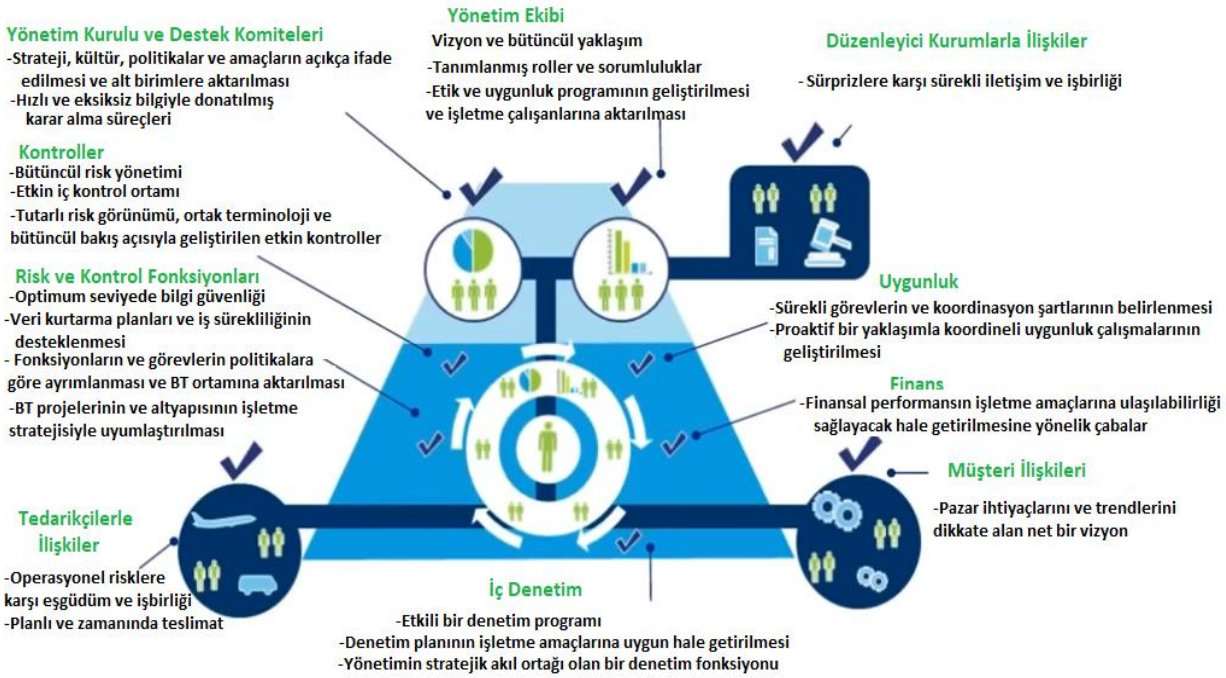
- Belirlenen sorunların, endişelerin ve fırsatların önem derecesine göre çözümü için, belirlenmiş yordamları ve destekleyici teknolojiyi kullanarak, bazı durumlarda bunların otomatik olarak çözümlenmesini sağlayan yolları tanımlayın ve uygulayın.

- Süreçleri yönlendirmekte ve her bir sorunun çözümünde denetim izinin takip edilmesini sağlamakta kullanılan, kilit çalışan ve araçların belirli olduğu araştırma ve sorun çözme yordamlarını geliştirin.
- Gerektiğinde ve uygun olduğunda iç ve dış paydaşlara zamanında raporlama yapılmasını sağlayın.
- Sorun çözme süreçleri boyunca alınan bilgiyi değerlendirin ve kontrollerin gerektiği gibi kurulmasında kullanın.

### 3.9.3. YRU Yaklaşımının Sağladığı Etkin İç Kontrol Ortamı

Bir işletme iş amaçlarına doğru ilerlediğinde ve bunlara ulaşmak için bir iş modeli uyguladığında, başarılarının önündeki engelleri ele almalıdır. İşletme, eylemlerinde sınırlamaların olduğunun da farkında olmalıdır. Elbette ki yasal sınırlar önemlidir, ancak işletmeler savundukları değerler ya da içinde bulundukları piyasa şartlarının dayattığı koşullardan kaynaklanan kendi gönüllü sınırlarıyla da karşı karşıyadırlar. Neyse ki, bir işletme amaçlarına doğru ilerlerken, iç kontrol süreçlerinin yardımını hesaba katabilir. Birçok önde gelen işletme, iç kontrol süreçlerinin muazzam miktarda birbiriyle çakıştığını keşfetmektedir. İşletme faaliyetlerinde etkinlik ve verimlilik ancak kontrol süreçlerinin bir bütün olarak ele alınmasıyla başarılabilir. Bunu da ancak YRU yaklaşımının getirdiği yeni iç kontrol ortamı sağlayabilir (Jackson, 2007, s. 51).

YRU yaklaşımı yönetişim, risk yönetimi ve uygunluk bileşenlerinin bütüncül bir bakış açısıyla yönetilmesini ve ilişkili süreçlerin etkin bir şekilde yürütülmesini sağlamanın yanı sıra, organizasyonun yönetimi ve iç kontrolünde konumlanan farklı fonksiyonlar arasında iletişim ve işbirliğini teşvik eden bir yönetim modelidir. YRU yaklaşımının sağladığı standartlaştırılmış dil ve tanımlar, karar alma süreçleri için sağladığı tutarlı ve eksiksiz bilgi ve özellikle risk ve kontrol fonksiyonları açısından iş süreçlerinin ve sorumlulukların işletme stratejileri, politikalar ve zorunlu sınırlara uygun olarak düzenlenmesinin önündeki belirsizliği ortadan kaldırması, işletmede etkin iç kontrolün geliştirilmesini kolaylaştıracaktır. Şekil 3.20, organizasyonun iç kontrolünde konumlanan farklı fonksiyonların bütüncül bakış açısı, ortak dil ve altyapıyla geliştirdiği etkin iç kontrolü tasvir etmektedir.




**Şekil 3.20.** *YRU Yaklaşımının Farklı Fonksiyonları Bütünleştirmesi (OCEG, 2018)*

İşletme fonksiyonları arasında eşgüdüm, işbirliği ve iletişim sonucunda işletmenin tamamı eksiksiz olarak değerlendirilir ve birbiriyle çakışan gereksiz çabaların önüne geçilir. Güvence boşluklarının veya güvence yorgunluğunun giderilmesiyle gereksiz kontrol maliyetleri veya hata, hile ve aksaklıkların ortaya çıkardığı zararlara katlanılmaz ve işletmenin tamamını kapsayan kontrol ortamı kurulur. Ortak terminolojiyle hazırlanmış raporların sunduğu eşsiz bilgi, birim yöneticilerine ve üst yönetime hataları, hileleri, değişimleri ve müdahaleleri daha hızlı tespit etme, tepki geliştirme ve etkin kontrol noktaları kurma fırsatı sunar. İşletmede kontroller, üst yönetimin strateji geliştirme sürecinden ve risk değerleme faaliyetlerinden bağımsız olarak değerlendirilmemelidir.

Üst yönetim, YRU yaklaşımının sağladığı yönetişim ve uygunluk çabalarıyla bütünleşmiş kurumsal risk yönetimi faaliyetlerinden elde ettiği risk bilgisini, işletme amaçları ve stratejileriyle uyumlaştırmalı, iç ve dış şartlara ve işletme ihtiyaçlarına uygun iç kontrolü tasarlamalıdır. YRU yaklaşımının sağladığı tutarlı bilgi, üst yönetimin ve fonksiyonel yöneticilerin, işletme birimlerinin faaliyetlerini daha doğru değerlendirmesini ve işletme amaçları ve stratejilerine yönelik performansın gösterilip gösterilmediğini anlamalarını sağlar. Ayrıca risk bilgisi, kaynakların doğru alanlara aktarılarak optimum şekilde kullanılması konusunda üst yöneticilere yol gösterir.

Organizasyon içinde YRU yaklaşımı doğrultusunda güçlü kontrollerin geliştirilmesini sağlamak için, yöneticiler aşağıdaki soruları tartışmalıdır (Hirth, 2008, s. 49):

- Hangi faaliyetler bugün ve gelecekte organizasyonun iç kontrolünü iyileştirir?
- Kontrollerin etkinliğini zaman içinde nasıl geliştirebiliriz?
- İşletmenin iç kontrolünü destekleyen ve tamamlayan bir düşünce yapısı ve kültürünü nasıl oluşturur ve koruruz?
- Organizasyonda etkin bir iç kontrol ortamını kurmak ve devam ettirmek için işletme yöneticileri nasıl konumlandırılmalı ve hangi sorumluluklar verilmelidir?

Bir işletmede etkili bir iç denetim faaliyetinin yürütülmesi, bu soruların cevaplanması ve iç kontrol amaçlarına ulaşılması konusunda yönetime destek olacaktır. Yönetim kurulu ve üst yönetimin tanımladığı stratejiler, amaçlar ve beklentilerle uyumlu hareket eden ve işletme dünyasının değişen ihtiyaçlarını dikkate alan faaliyetler yürüten güçlü bir iç denetim fonksiyonuna sahip işletmeler, genellikle daha iyi kontrollere sahiptir. Güçlü bir iç denetim fonksiyonunun varlığı, işletmenin kontrol ortamında YRU yaklaşımının savunduğu iletişim ve işbirliği kültürünün geliştirilmesini hızlandıracak ve kolaylaştıracaktır.

Günümüz iç denetçilerinin, organizasyonlarının iç kontrol yapısını kurmak ve sürekli iyileştirmek için yönetişim, risk yönetimi ve uygunluk ile ilgili çeşitli zorluklarla baş edebilecek yenilikçi bir düşünce yapısına sahip olmaları gereklidir. İç denetçilerin ortaya çıkan risk faktörlerini tespit etmek, değerlemek ve kontrol altına almak, işletmelerinin gereksinim duyduğu yeni teknolojileri keşfetmek ve karmaşık işletme problemlerine yaratıcı çözümler üretmek amacıyla sürekli olarak kendilerini geliştirmeleri ve her zaman hazır olmaları gereklidir. Böylece iç denetçiler, işletmelerinin YRU girişimlerine gözetim ve güvence sağlayabilecekleri, işletmelerinin iç kontrolüne daha fazla değer katabilecekleri ve gerekli gördüklerinde sorumluluklarının kapsamını genişletebilecekleri proaktif bir pozisyona sahip olacaklardır (Hirth, 2008, s. 50).

### 3.10. YRU'nun İş Performansı Üzerindeki Etkisi

YRU yaklaşımının işletmede benimsenmesi iş performansının geliştirilmesine katkı sağlar. YRU'nun işletmeye sağladığı faydalar işletme faaliyetlerine daha düşük maliyetle güvence sağlanması, etkin iç kontrollerin geliştirilmesi ve aksaklık, hata ve kayıpların önlenmesi gibi doğrudan iş performansı üzerinde olumlu etkiler yaratır. Ayrıca YRU'nun bütüncül bakış açısı doğru teknolojiyle desteklendiğinde, performans daha doğru ölçülebilir ve düşük performanslı alanlar geliştirilebilir.

#### 3.10.1. Güvence sağlama maliyeti

YRU'nun uygulanması, çalışanlara birbirlerinin işlerini anlama ve böylece birbirlerinin işlerine güvenme fırsatı sunar. İşletme içindeki birim yöneticilerinin yaygın şikâyeti; iç denetçilerin, risk yöneticilerinin ve uygunluk çalışanlarının birbirinden bağımsız çalışmaları ve bu yüzden işlerinin birbirini tekrar etmesi veya kısmen ortak faaliyetlerin yürütülmesidir. Örneğin iç denetçiler operasyonel risk çalışanları tarafından kullanılanlara çok benzeyen (hatta aynı) hile soru formları kullanıyor olabilirler. Her iki birimin çalışanları işletme içindeki diğer çalışanlara aynı soruları soruyor olabilirler. İki birimin çalışanları birbirlerinin işlerini tekrarladıklarında bu durum toplanan verilerin hem iç denetçiler hem de risk çalışanları tarafından belgelendirilmesi ve analiz edilmesiyle hem de çalışanların iki kere zaman harcamalarıyla maliyet israfına yol açmaktadır. YRU yaklaşımı, söz konusu güvence çalışanlarının birbirlerinin işlerini olabilecek en üst düzeyde paylaşmalarına izin veren bir çerçeve sunarak güvence maliyetlerini azaltır.

#### 3.10.2. İç kontrol maliyeti

YRU yaklaşımının uygulanması iç kontrol maliyetlerinin aşağıya çekilmesini sağlar. İşletme çapında ortak bir şekilde uygulanan kontroller tanımlanır ve bunlara güven duyulur. İşletme çapındaki kontroller işlem ve süreç seviyesindeki kontrollerin yerini almalıdır. Kontroller işbirliğiyle geliştirilebilir. Örneğin operasyonel risk çalışanları en önemli hile risklerini tanımlamışlarsa, sonrasında uygunluk çalışanları hileyi önlemek veya ortaya çıkarmak için tasarlanmış kritik kontroller tanımlayabilirler. Şayet hile ihlallerinin çoğunluğu, uygun şekilde eğitilmeyen çalışanların şüpheli işlemleri raporlamadaki yetersizliğinden kaynaklanıyorsa, mevzuata uyum eğitimi büyük olasılıkla etkin bir kontrol oluşturacaktır. Ayrıca günümüzde birçok durumda YRU çalışanları

riskleri azaltmaktan ziyade, risk bilgisinin olmadığı hallerde kontroller geliştirirler. Etkin YRU uygulamaları ve işbirliğiyle bunun önüne geçilebilir.

### 3.10.3. Kaza ve aksaklıkların maliyeti

YRU yaklaşımından ekonomik fayda sağlanabilecek alanların biri de kaza ve aksaklıklar gibi zarar oluşturan durumların önlenmesidir. Risk ve kontrol konusunda ortak bir dilin oluşturulmasıyla, çalışanlar neden-sonuç ilişkisine yönelik bir anlayış oluşturabilirler. Başarısızlıkların temel nedenleri ve sebep oldukları olayları ortaya koymak, kaza ve aksaklıkların azaltılmasında önemli bir bilgi kaynağı sağlayacaktır.

### 3.10.4. Performans göstergeleri yoluyla kazanılan maliyet

Mevcut güvence standartları ve uygulamalar, işletme performansını dikkate almaz ve güvence konusunda oluşturulan görüşler işletme performansıyla ilgili olmamaktadır. Örneğin, performans amaçlarına ulaşılmadığında dahi, iç denetçiler iç kontrol hakkında olumlu görüşler ifade edebilirler ya da risk çalışanları risklerin etkin bir şekilde yönetildiği kanısına sahip olabilirler. YRU yaklaşımının uygulanmasıyla genel çerçeve, değer yaratılması, yaratılan değerin korunması ve performansın geliştirilmesi doğrultusunda yönlendirilir. Bu çerçeveyi takip ederek, bütün YRU çalışanları kendi ulaştıkları sonuçların işletme performansı üzerindeki etkisi arasında doğrudan bir bağlantı kuracaklardır. Riskler, kontroller ve önlemler bunların işletme performansı üzerindeki etkilerine doğrudan bağlı olacaktır. Örneğin bir üretim faaliyetinin temel performans göstergesi, üretilen parçaların anında dağıtımını öngörüyorsa, riskler ve kontroller buna göre geliştirilecektir ve böylece maliyet tasarrufu sağlanacaktır.

## 3.11. YRU Yaklaşımında Teknolojinin Rolü

YRU kavramı, yeni bir işletme yönetimi felsefesi olmasının ötesinde denetim, risk yönetimi, uygunluk ve diğer ilişkili faaliyetleri yönetmek amacıyla geliştirilen ve ortak özellikler ile fonksiyonlar taşıyan bir yazılım sınıfını ifade etmek amacıyla da kullanılmaktadır. Kavram aynı zamanda birtakım profesyonel uygulamaları içerecek şekilde, özellikle YRU'nun kapsadığı alanların teknolojik dönüşümünü vurgulamaktadır. İç denetçilerin işletme içinde birçok YRU çalışanı ve yöneticisi tarafından da kullanılan bu teknoloji sınıfını anlamaları hem güvence hem de danışmanlık işlevi açısından büyük önem taşır (Adams vd., 2016, s. 49).

İşletmeler, YRU altyapısının temelini oluşturan çeşitli teknolojilerle karşılaşırlar. İşletme çalışanları, risk ve uygunluk teknolojileri satan BT sağlayıcılarının sunduğu ürün kalıplarına uymakta zorlanırlar. YRU yazılımlarının -işletmelere özel şekilde değiştirilmeden- bütün pazara uymaması aslında şaşırtıcı değildir. İşletmeler, teknoloji satıcılarına yaklaşırken, iç denetçiler, karar alıcılara işletmeyi etkileyen risk ve uygunluk ihtiyaçlarını göz önünde bulundurmalarını tavsiye etmelidir. İç denetim, işletme faaliyetleri için gereken ihtiyaçları en iyi şekilde karşılayan YRU yazılımını sunan teknoloji tedarikçisinin seçilmesini sağlamalıdır. Doğru teknoloji altyapısı, sürdürülebilir ve etkili bir YRU stratejisi için kilit bir etkendir (Rasmussen, 2009, s. 65).

Büyük, küçük, kamu ya da özel bütün işletmeler, süreçlerinde teknolojiyi kullanmalıdır. YRU bilgisinin BT ortamında ulaşılabilirliği, işletme yöneticileri ve çalışanları için büyük önem taşır. İç denetçilerin ve diğer ilgili çalışanların, YRU yazılımlarıyla ilgili bilmeleri gereken temel kavramlar şunlardır (Mitchell, 2007, s. 295):

- Temel Mimari: Temel mimari, işletim sistemleri ve ağ bağlantısı gibi güvenlik ve erişim kontrolleri şeklinde sıralanabilen temel hizmetleri sağlar. Bu teknolojiler YRU ihtiyaçlarını desteklemek için bütünleştirilebilme ve uyarlanabilmeyi sağlamak amacıyla ayrıntılı olarak incelenmelidir.
- Veri Hizmetleri: Veri hizmetleri, diğer birçok uygulamanın bağlı olduğu veri tabanı ve ilgili teknolojileri kapsar. Bu teknolojiler, ihtiyaçları desteklemek için iş süreçlerine uyarlanabilmek amacıyla ayrıntılı olarak incelenmelidir.
- Kurumsal Hizmetler: İşletme çalışanları iş akışı yönetimi, güvenlik yönetimi ve belge yönetimi gibi işletme fonksiyonları tarafından paylaşılan birçok kurumsal hizmetten faydalanır. Bu teknolojiler, YRU ihtiyaçlarını desteklemek için ayrıntılı olarak incelenmelidir.
- YRU Uygulamaları: Öncelikli olarak YRU'ya özel süreçleri desteklemek amacıyla var olan çok sayıda uygulama vardır. Risk, kontrol ve hesap verebilirliğe ilişkin amaçları planlayan, kontrolleri izleyen, sorunları yöneten veya yardım hatlarını etkinleştiren otomatik teknolojiler bu uygulamaların başında gelir. Bu teknolojiler sadece YRU'ya özel işlemleri yürütmez. Ancak önemli ölçüde YRU uygulamalarına yöneliktir.

### 3.11.1. YRU Yazılımları

Günümüzde Yönetim Bilişim Sistemi (YBS) olarak nitelendirdiğimiz olgu, bilgi sistemlerinin oluşumu, karşılıklı etkileşimleri, alt sistemlerin birbirini inşası ve tamamlamasıyla oluşmuştur. Muhasebe Bilgi Sistemi (MBS) açısından, teknolojik keşifler ve gelişmeler, bilgisayar sistemlerinin evrimleşerek Bilgi Teknolojilerine dönüşmesini ve MBS-YBS-BT örtüşmesine neden olmuştur (Erdoğan, 2017, s.747). İşletme ihtiyaçları, bilgi sistemlerinin teknolojik dönüşümünün temel güdüleyicisidir. Üretim veya stok maliyetlerinin ağırlık kazandığı dönemde Malzeme İhtiyaç Planlama (MRP), dağıtım ve lojistik faaliyetlerin öneminin artmasıyla Dağıtım İhtiyaç Planlama (DRP), rekabet üstünlüğünün müşteri ve tedarikçilerle ilişkilerden geçtiğinin anlaşılması Müşteri İlişkileri Yönetimi (CRM) ve Tedarik Zinciri Yönetiminin (SCM) ortaya çıkmasına yol açmıştır. Bu dönüşümün en önemli dönüm noktalarından biri, tedarik, üretim ve dağıtım kaynaklarının verimli kullanılmasını sağlamak amacıyla farklı işletme ihtiyaçlarına cevap vermek için tasarlanan modüllerden oluşan bütünleşik bir yönetim sistemi olarak tanımlanan Kurumsal Kaynak Planlamasının (ERP) geliştirilmesidir. ERP, internetin ve ileri teknolojilerin kullanımı ve CRM, SCM, Kurumsal Performans Yönetimi (CPM) ve İşletme Zekâsı (BI) gibi kavramların devreye girmesiyle ERP 2 noktasına ulaşmıştır.

Yönetişim, risk yönetimi ve uygunlukla ilişkili işletme çabalarının birlikte ele alınması ve değerlendirilmesi ihtiyacı önce YRU kısaltmasıyla ifade edilmiş, sonrasında söz konusu işletme faaliyetlerine denetim, kontrol, performans yönetimi, etik, kalite yönetimi gibi diğer ilişkili faaliyetlerle bütünleşik şekilde ve bütüncül bir bakış açısıyla yönetilmesi gerektiği felsefesini savunan YRU yaklaşımına dönüşmüştür. YRU yaklaşımının savunduğu ortak terminoloji, ortak süreçler, örgütsel yapı ve yönetim kültürü; işletme üst yönetimi, çalışanlar ve birim yöneticileri tarafından ancak YRU yazılımlarının sağladığı teknolojik altyapıyla hayata geçirilebilir. YRU yazılımları işletmelerin YBS'ini oluşturan diğer yazılımlarla özellikle ERP ile bağlantılı olarak çalışır. Başlıca YRU teknoloji sağlayıcıları ve yazılımları şunlardır:

SAP-GRC, RSA Archer-eGRC, Oracle-GRC Manager, MetricStream-MetricStream IT GRC, ACL-GRC, Parapet-Integrated Risk Management, ProcessGene-GRC, Continuity Partner-TrackMyRisks, SAI Global-Compliance 360, IRM Security-SYNERGi GRC Platform, GBTEC Software-BIC Cloud GRC, BWise-BWise GRC Platform, Compass IT Compliance- Compass IT GRC, Symmetry-ControlPanelGRC,

Dion Global Solutions-GRC Enterprise, Risma Systems- GRC Software, SAS Institute-SAS Governance and Compliance Manager, DDi-Tula Oversight, Nasdaq BWise- GRC.

Sürekli değişen koşullar, ortaya çıkan yeni risk faktörleri ve sürekli değişen zorunlu veya gönüllü düzenlemeler, söz konusu faaliyetlerin Microsoft Excel veya Access gibi basit ofis programlarıyla takip edilmesini ve ölçülmesini imkânsızlaştırmıştır. İşletmeler YRU yazılımlarıyla, şemsiye bir kavram olan YRU kısaltmasının arkasında bulunan tüm faaliyetlere ilişkin bilgiyi, işletme yazılımlarından, iç raporlardan, ilgili yasal düzenlemelerden veya diğer dış raporlardan ve işletmenin faaliyet gösterdiği sektöre özgü ölçümlerden izleyebilecektir. Böylece, Endüstri 4.0 Devrimi sonrası dönemde, işletmeler için bir seçenek olmaktan çıkıp bir zorunluluk haline gelen sürekli güvence (Yıldız, 2019, s. 99), hayata geçirilmesi için kullanılması gereken teknolojilerle birlikte daha etkin ve düşük maliyetle sağlanabilecektir.

Endüstri 4.0 Devrimini yaratan teknolojilerin keşfi, işletme faaliyetlerine ilişkin iç ve dış kaynaklı yapılandırılmış, yarı yapılandırılmış veya yapılandırılmamış verinin karar süreçlerinde değerlendirilebilmesini sağlamıştır. YRU yazılımlarıyla elde edilen tutarlı risk ve kontrol bilgisinin, güvence çalışanları tarafından büyük veri analitiği ve makine öğrenmesi algoritmalarıyla analiz edilmesi, daha güçlü kontrol noktaları geliştirmelerini ve gelecekteki olaylara ilişkin öngörü elde etmelerini sağlayacaktır. Diğer taraftan, işletmeyi çevreleyen risklerin 7 gün 24 saat aralıksız tehdit oluşturması, sürekli güvencenin bileşenleri olan sürekli kontrole ve sürekli risk değerlemeye ihtiyaç duyulan bir ortam yaratmıştır (Yıldız, 2019, s. 98). YRU yazılımlarının üst yöneticilere ve iç denetçilere sağladığı bütüncül risk görünümü ve tutarlı bilgi, veriden öğrenebilen ve performansı öğrenmeyle artan makine öğrenmesi algoritmaları veya çeşitli faaliyetleri insana benzer şekilde yapabilen yapay zekâ teknolojileri aracılığıyla etkin kontrollerin geliştirilmesinde kullanılabilir.

YRU yaklaşımı, üst yönetime ve yönetim kuruluna karar süreçlerinde gereken özellikle işletme içi raporların ilgili tüm fonksiyonların eşgüdümü ve işbirliğiyle hazırlanması gerektiğini ve böylece karar süreçlerinde önemli bilginin dikkate alınmasını engelleyen bir rapor karmaşası yaşanmaması gerektiğini savunur. YRU yazılımları Yönetim Bilişim Sisteminde mevcut ERP gibi diğer yazılımlardan ihtiyaç duyulan verinin elde edilmesini ve sorumluluk sınırlarının belirlenerek raporların fiziksel olarak bir araya gelinmese bile, sorumluluk sınırlarına uygun işbirliği ve eşgüdümle hazırlanmasını sağlayan teknolojik altyapıyı sunar. YRU yazılımlarının sağladığı bütünleşik raporlama

altyapısı, özellikle farklı modüllerden ve işletme fonksiyonlarından bilgi elde edilmesini gerektiren ve finansal olmayan bilgiyi finansal bilgiyle bir araya getiren sürdürülebilirlik raporlarının ve entegre raporların çok daha hızlı, kolay ve düşük maliyetle hazırlanmasını sağlar.

YRU yaklaşımı ortak çerçeve, dil ve bütüncül bakış açısıyla, işletmenin farklı fonksiyonlarını etkileyen tehditlere karşı çeşitli risk faktörlerinin etkisini ölçümleyen bütüncül risk bilgisinin elde edilmesini sağlar. YRU yazılımları, dış ve iç şartlara göre üst yönetimin tasarrufunda olan, işletmenin kendi politika ve stratejilerinden kaynaklanan gönüllü sınırların ve sürekli değişen ekonomik konjonktürden ya da işletmenin uymakla mükellef olduğu dış düzenlemelerden kaynaklanan zorunlu sınırların izlenmesini sağlar. YRU yazılımları, ortak bir çerçeveye bağlı kalınarak, geleneksel kontrol taksonomisinin ötesinde daha proaktif bir anlayışla geliştirilen kontrollerin, BT ortamında uygulanmasını sağlayan teknolojilerin kullanılabilmesini sağlar. YRU yazılımları, risk ve kontrol açısından aşağıdaki temel faydaları sunar (Pehlivanlı, 2015, s. 168):

- Görevlerin ayrılığı ilkesine uyum, gerçek zamanlı olarak izlenebilir.
- Erişim riskleri, şeffaf bir şekilde izlenebilir ve önleyici kontrol mekanizmaları işletilebilir.
- Merkezileştirilmiş denetim belgelendirmesi yürütülebilir.
- Manuel kontrollerin amaçlandığı gibi otomatikleştirilmesini kolaylaştırır.
- Kontrollerin işletme amaçlarına uygun işlemesine yönelik optimizasyonu sağlar.
- Kontrol ilkelerine uyumun güvence çalışanları tarafından değerlendirilmesine imkan verir.
- Kontrol testleri ve belgelendirmeye yönelik merkezi raporlama altyapısını sunar.
- Birçok iç ve dış faktörden etkilenen uygunluk çerçevesini işletme süreçleriyle bütünleştirir.
- Risklerin anahtar risk göstergeleriyle (KRI) proaktif olarak izlenmesini sağlar.
- İç denetim, iç kontrol, risk yönetimi, uygunluk, BT ve hukuk fonksiyonları tarafından bilginin değerlendirilmesi süreçlerini bütünleştirir ve zaman-maliyet tasarrufu sağlar.
- Sürekli izleme altyapısı sunar.
- Kontrol testlerinin otomatik ve sürekli yürütülmesini sağlar.
- Kontrol ve iç denetim maliyetlerini, sağladığı bütünleşmeyle azaltır.

- Risk yönetimini yönetişim ve uygunluk ile koordineli çalışan bir yapıya kavuşturur.
- İşletmenin maruz kaldığı çeşitli riskleri konsolide eder.
- Tüm işletme fonksiyonlarını ve ihtiyaçlarını dikkate alan bir risk yönetimi tutumu geliştirilmesini sağlar.
- Karar alma süreçlerinde stratejilerin ve işletme amaçlarının risklerle ilişkilendirilmesini sağlar.

### 3.11.2. OCEG Bilgi Teknolojileri Rehber ve İlkeleri

YRU yazılımlarının birincil amacı, işletme amaçları ve kurumsal yönetişimle en yakından ilişkili olan risk yönetimi, güvence ve uygunluk faaliyetlerinin raporlama ve belgelendirme süreçlerini otomatikleştirmektir. YRU yazılımlarının temel kullanıcıları, denetim komiteleri, sorumlu üst yöneticiler, iç denetçiler, risk ve uygunluk çalışanları ve yöneticileridir. İşletmeleri YRU yazılımlarına yönlendiren temel sebepler, işletme fonksiyonları arasında YRU yaklaşımının savunduğu ortak taksonomi, terminoloji ve stratejilerin geliştirilmesi ve işbirliği kültürünü destekleyen raporlama altyapısının sağlanması ihtiyaçlarıdır. YRU yazılımları, risk ve uygunluk verisinin kalitesini artırır ve yönetimini kolaylaştırır, risk teknolojilerinin değişen düzenlemelere adaptasyonunu sağlar ve zamanında raporlama yapılabilmesini sağlar (Cau, 2014, s. 31).

OCEG'in kırmızı kitap olarak isimlendirdiği ana çerçevesi sekiz temel unsurdan oluşur. Tablo 3.9'da verilen, YRU yetenek modelinin unsurlarından sonuncusu olan bilgilendirme ve bütünleşmenin alt unsurları, YRU teknolojilerinden nasıl amaçlandığı şekilde faydalanılacağının sınırlarını çizer (OCEG, 2009, 2015):

**Tablo 3.9.** *Bilgilendirme ve Bütünleşmenin Alt Unsurları (OCEG, 2015)*

| |
|---|
| **I -Bilgi ve Bütünleşme** |
| **1. Belge Yönetimi ve Dokümantasyon** |
| 1.1. Bilgi yönetimi sınıflandırma yapısının geliştirilmesi |
| 1.2. Bilgi toplama politika ve yordamlarının geliştirilmesi |
| 1.3. Bilgi kullanımı ve transferi politika ve yordamlarının geliştirilmesi |
| 1.4. Bilgi depolama politika ve yordamlarının geliştirilmesi |
| **2. İç ve Dış İletişim** |
| 2.1. Raporlama planının yapılması |
| 2.2. İletişim planının yapılması |
| **3. Teknoloji ve Altyapı** |
| 3.1. Teknoloji ihtiyaçlarının ve bağlantı boşluklarının değerlendirilmesi |
| 3.2. Stratejik YRU planında teknolojik amaç ve stratejilerin geliştirilmesi |

YRU yaklaşımının savunduğu fonksiyonlar arası bütünleşmenin sağlanması için gereken teknolojik altyapının oluşturulması için hata, eksiklik ve kopuklukların giderilmesi, işbirliği için ihtiyaç duyulan raporlama hatlarının geliştirilmesi ve faaliyetler üzerinde riskin ölçülmesi ve etkin kontrollerin kurulmasını sağlayan teknolojilerden stratejik olarak faydalanılmasına imkân sağlayan teknolojik altyapının geliştirilmesi YRU yetenek modelinin (bilgi ve bütünleştirme unsurunun) odak noktasıdır.

OCEG, Teknoloji Çözüm Rehberinde, YRU yaklaşımının altyapısı olarak tanımlanan teknolojik çözümlerin geliştirilmesi amacıyla üst yönetim, BT uzmanları, iç denetçiler, risk ve uygunluktan sorumlu yöneticilerin temel olarak şu adımların atılması için çaba göstermeleri gerektiğini tavsiye etmektedir (OCEG, 2015c):

- Örgütün YRU ihtiyaçlarını gideren teknolojilerin belirlenmesi için tutarlı politikalar uygulanmalıdır.
- Bilgi paylaşımı ve işbirliğini destekleyen teknolojik altyapı kurulmalıdır.
- Bilginin tutarlılığını garanti eden ve risk, kontrol ve izleme faaliyetlerini destekleyen teknolojilerden faydalanılmalıdır.
- Amaçlara ulaşmak için birey ve takım sorumlulukları belirlenmelidir.
- Risk ve uygunluk sorumluluklarının üstlenilmesine ilişkin hesap verebilir karar süreçleri geliştirilmelidir.
- Yönetim, YRU ihtiyaçlarının teknoloji desteğiyle çözülmesine ilişkin amaçları açıkça belirlemelidir.
- Risk ve uygunluk bilgilerinin doğru, eksiksiz ve zamanında ulaşılabilmesini sağlayan altyapı oluşturulmalıdır.

OCEG Teknoloji Çözüm Rehberinde, 28 YRU teknoloji çözümü kategorisini sınıflandırmıştır. İşletmenin özelliklerine, ölçeğine ve faaliyet gösterdiği sektöre göre günümüz bilgi teknolojileri dünyasında tanımlanan kategorilerin tamamında ya da büyük çoğunluğunda teknolojik çözümlerden faydalanması gereklidir (OCEG, 2015c):

**Tablo 3.10.** *OCEG'in 28 YRU teknoloji çözümü (OCEG, 2015c)*

| |
|---|
| BT.01 Denetim ve Güvence Yönetimi |
| BT.02 Yönetim Kurulu ve Kurumsal Yönetim |
| BT.03 Marka ve İtibar Yönetimi |
| BT.04 İş Sürekliliği Yönetimi |
| BT.05 Uygunluk Yönetimi |
| BT.06 Sözleşme Yönetimi |
| BT.07 Kontrol Faaliyetleri, İzleme ve Güvence |
| BT.08 Kurumsal Sosyal Sorumluluk |
| BT.09 Keşif/Soruşturma Yönetimi |
| BT.10 Çevresel İzleme ve Raporlama |
| BT.11 Çevre, Sağlık ve Güvenlik |
| BT.12 Finansal/Fon Risk Yönetimi |
| BT.13 Hile ve Suiistimal Tespiti, Önleme ve Yönetimi |
| BT.14 Küresel Ticaret Uygunluğu/Uluslararası İlişkiler |
| BT.15 Acil Yardım/Destek Hatları |
| BT.16 Bilgi Teknolojileri Risk ve Güvenliği |
| BT.17 Sigorta ve Hasar Yönetimi |
| BT.18 Fikri Mülkiyet Yönetimi |
| BT.19 Sorun ve Adli Soruşturmalar Yönetimi |
| BT.20 Sorun Yönetimi |
| BT.21 Fiziksel Güvenlik ve Kayıp Yönetimi |
| BT.22 Politika Yönetimi, İletişim ve Eğitim |
| BT.23 Bilgi Gizliliği Yönetimi |
| BT.24 Kalite Yönetimi ve İzleme |
| BT.25 Raporlama ve Bilgilendirme |
| BT.26 Risk Yönetimi |
| BT.27 Strateji, Performans ve İş Zekâsı |
| BT.28 Üçüncü Taraf/Tedarikçi Riski ve Uygunluğu |

### 3.11.3. YRU Teknolojilerinin denetimi

İç denetçiler hali hazırda bilgi teknolojilerini anlamak ve güvence sunmak için gerekli çerçeve ve standartlara sahiptirler. İç denetim faaliyetlerinde asıl önemli olan YRU teknolojilerinin anlaşılmasıdır. YRU teknolojileri olarak tanımlanan araçlar ve uygulamalar, tüm ilgili çalışanların hizmetine sunulmuştur. İç denetim faaliyetinin esas odaklanması gereken sorumluluk, işletme yöneticileri ve çalışanlar tarafından güven duyulan teknolojiye ve sisteme yönelik güvence sunulmasıdır (Adams, 2016, s. 51).

Bilgi teknolojileri denetimi kısaca; "*BT'nin finansal tablo üretimini gerçekleştirmek için gereksindiği ve kullandığı, yönetim bilgi sisteminin bütünleşik yapısında çok farklı ve çeşitli noktalarda yer alan, finansal ve operasyonel işletme süreçlerinin tümünü içeren bilgi işleme uygulamalarının denetlenmesi*" olarak tanımlanabilir (Erdoğan, 2012, s.112).

Denetimin temel felsefesi düşünüldüğünde YRU teknolojilerinin denetimi, BT denetiminden farklı bir olgu değildir. Esas farklılık, YRU teknolojilerinin işletmenin güvence çalışanlarına sağladığı ortak denetim evreni gibi faydaların, geleneksel bilgi teknolojilerine kıyasla denetim faaliyetlerini çok daha kolay ve verimli hale getirmesidir. YRU yaklaşımını benimseyen bir işletmede uygulamaların birçoğu artık BT ortamında yürütülmektedir. YRU ortamında yapılacak bir denetim, tıpkı normal bir BT denetiminde olduğu gibi, öncelikle YRU teknolojilerinin yapısını anlamakla başlamalıdır. İç denetçilerin YRU teknolojilerinin özelliklerini keşfetmesi, denetimin planlanması ve yürütülmesinde işlerini kolaylaştıracak ve verimliliği artıracaktır. YRU teknolojilerinin güvence çalışanlarına sağladığı faydalar ve desteklediği güçlü iç kontrol yapısı, iç denetim faaliyetlerinin daha hızlı, anlaşılır, eşgüdüm içinde ve verimli yürütülmesini sağlayacaktır.

### 3.11.4. Teknolojinin YRU Faaliyetlerine Etkileri

Yakın zamanda çalışanların gereksinim duyduğu ve haklarında güvence sunacakları bilgilerin elektronik kayıtlar halinde veri tabanlarında bulunacağını söylemek hiç de abartılı olmaz. Birçok işletme çalışanının görevi, bilginin bulunması, düzenlenmesi ve bunlardan yeni bilgiler üretilmesi olacaktır. Teknolojik gelişmeler, YRU yaklaşımının uygulanabilmesinde önemli bir etkendir. Çok büyük boyutlardaki yapılandırılmış, yarı yapılandırılmış veya yapılandırılmamış verinin bir araya getirilmesi ve yönetilmesi ile bilginin işletme çapında ve özellikle risk ve güvence çalışanları arasında paylaşılabilmesi, YRU'yu işletme için otomatik olarak çalışan bir sistem haline getirir. Teknolojinin sağladığı başlıca katkılar şöyle sıralanabilir (Adams vd., 2016, s. 49):

- Teknoloji bilgiyi sınıflandırmakta, paylaşılmasına imkân sağlamakta ve ayrıntılı bilgi kümelerinin oluşturulmasına izin vermektedir. Örneğin bir fonksiyonun iç denetim raporunun; işe yönelik risk yaklaşımı, çalışanların yeterlikleri ve işten ayrılma oranları gibi insan kaynakları bilgisi ve yasalara uygunluk performansı gibi farklı değerlendirmeler içermesi sağlanabilecektir. Yığınlar halinde bulunan ve daha önce paylaşılamayan bilgi, teknolojiler ve ileri analitik araçlar ile artık kolayca bir araya getirilebilmekte, sınıflandırılabilmekte ve belli başlıklar altında analiz edilebilmektedir.
- Birbiriyle uyumlu iş akışları ve yordamlar oluşturulabilir ve izlenebilir. Riskler işletme çapında aynı biçimde tanımlanabilmekte ve değerlendirilebilmektedir.

Kontroller, ortak ve ilişkili test stratejilerine tabi olabilmektedir. Birbiriyle uyumlu bir şekilde geliştirilmeleri nedeniyle risk ve kontrol değerlendirmeleri kolayca bir araya getirilip, karşılaştırılabilmektedir.

- İş performansı, işletme çapında bütüncül bir bakış açısıyla izlenir ve gerçek zamanlı olarak kaydedilir. Risk eylemlerinin ve kontrollerin etkinliği için iş performansı bir gösterge olarak kullanılabilir. Aynı şartlara tabi olan ve buna karşın yüksek başarı yakalayan grupların iyi risk yönetimi ve kontrollere sahip oldukları düşünülebilir.
- Standartlaştırılmış iş akışlarıyla birleştirilmiş bilgi toplama araçları, başarısızlıkların temel sebeplerini açıklıkla ortaya çıkarır. Hileler, iş kesintileri, hatalar ve aksaklıklar otomatikleştirilmiş süreçlerle izlenebilir ve analiz edilebilir.
- YRU çalışanları ortak bir güvence evrenini paylaştıkları için çok daha iyi ve koordine edilmiş bir kaynak tahsisi mümkün hale gelir.
- Teknoloji, finansal raporlama ve diğer göstergeleri büyük çapta geliştirebilir.
- Kontrollerin etkinliğinin iş performansı üzerindeki etkisinin incelenmesiyle çok daha etkili iç kontrolün geliştirilmesi sağlanır. İzleme gibi yukarıdan aşağıya yapılan kontroller, süreç temelli kontrollerin yerini alır.
- Teknoloji kullanarak öz değerlendirme ve anketlerini (risk ve kontrollerin tanımlanması, değerlenmesi, ölçülmesi ve izlenmesi sürecinde kullanılan anket, çalıştay, beyin fırtınası ve görüşme gibi tekniklerle yapılan bir çalışmadır) kapsayan işbirliği ve ortak çalışma, çok daha kolay hale getirilebilir. Öz değerlendirme ve anketler, risk ve kontrol değerlendirmelerine çok daha fazla tutarlı bilgi sağlanmasına destek olur.
- Sürekli izleme teknolojiyle mümkün hale getirilebilir.[8]

Teknoloji altyapısı, YRU girişimlerinin tasarlanmasını ve yönetilmesini kolaylaştırır. Teknoloji, iş süreçlerinin bilgi teknolojileri ortamında işletme amaçlarıyla tutarlı, sürdürülebilir ve bütünleşik olarak yürütülmesini mümkün hale getiren çeşitli kullanımı kolay uygulamalar sağlayabilir. Uygun teknolojik altyapının sağladığı faydalar, aşağıda sıralanan yönetişim, risk yönetimi ve uygunluk faaliyetlerinin çok daha etkili ve verimli olarak yerine getirilmesi potansiyelini geliştirir (Switzer vd., 2013, s. 12):

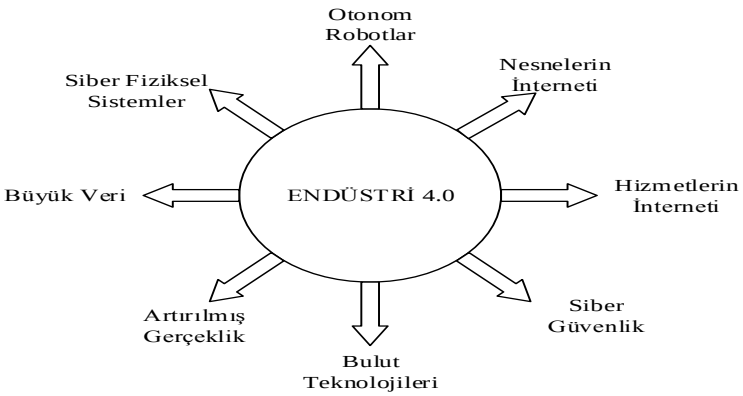
- İşletme amaçlarına yönelik düzenlenmiş risklerin merkezi bir görünümü sayesinde daha güçlü ve stratejik karar alma,

[8] Teknolojinin YRU yaklaşımına faydaları konusunda bakınız: https://www.sap.com/solution/platform-technology/analytics/grc.html

- İş planlama ve karar alma süreçleri ile risk ve uygunluk yönetimini bütünleştirme,
- Etkili risk yönetimi sayesinde performans optimizasyonu için fırsatları tanımlama,
- Riski daha erken tespit etme, daha iyi kontrol altına alma ve gerçek zamanlı görünürlük ile riske maruz kalmayı azaltma,
- Güçlü yönetişim pratikleriyle marka ve işletme itibarını güçlendirme ve hissedar değerini koruma,
- Düzeltilmiş süreçler ve rasyonelleştirilmiş kontrollerle kaynaklardan daha doğru faydalanma ve verimliliği geliştirme.

### 3.11.5. Endüstri 4.0 Unsurlarının YRU Faaliyetlerine Etkileri

İlk defa 2011 yılında Hannover Fuarında kullanılan bir kavram olan Endüstri 4.0, üretim araçlarının birbiriyle iletişim kurabildiği ve otonom hareket edebildiği, ileri teknolojilerle kuşatılmış, emek yoğun üretimden insan hatalarının minimuma indirildiği makine yoğun üretime dönüşümünü savunan; birçok modern otomasyon sistemini, veri transferi araçlarını ve üretim teknolojilerini kapsayan kolektif bir terimdir. Bu devrim temelde Nesnelerin İnterneti, Hizmetlerin İnterneti ve Siber-Fiziksel Sistemlerin birlikte çalışmasını öngören bir değerler bütünüdür. Nesnelerin İnterneti veya Hizmetlerin İnterneti ile Siber-Fiziksel sistemler birbirleriyle ve insanlarla gerçek zamanlı olarak iletişime geçip işbirliği içinde çalışabilecektir. 4. Sanayi Devrimiyle ortaya çıkan ileri teknolojilerle donatılmış kolektif çalışma ortamının unsurları şekilde gösterilmiştir (Erdoğan, 2017, s.7).




**Şekil 3.21.** *Endüstri 4.0 Unsurları (Erdoğan, 2017, s. 7)*

Endüstri 4.0 devriminin unsurları olarak tanımlanan Nesnelerin İnterneti, Otonom Robotlar, Bulut Teknolojileri, Artırılmış Gerçeklik ve Siber Fiziksel Sistemler gibi keşifler; işletmelerin iş süreçleri ve kontrol ortamı üzerinde çok büyük dönüşümlerin yaşanmasına sebep olmuştur. İşletme yöneticileri, Endüstri 4.0 unsurlarının kullanımı sayesinde, çok daha etkin ve verimli iş süreçleri ve kontrol ortamları geliştirebileceklerinin farkına varmışlardır:

- Otonom robotlar ve ileri teknolojik araçlar sayesinde işletme faaliyetlerin tamamen otomatikleştirilmesi ve insan hatasından arındırılması sağlanabilir. Çalışan kontrollerinin yerine istenmeyen durumların yaşanması halinde veya yöneticiler tarafından belirlenen sınırların aşılması halinde sistemi uyaran ve düzgün çalışmasını sağlayan otomatik kontroller geliştirilebilir.
- Nesnelerin ve Hizmetlerin İnternetiyle Siber Fiziksel Sistemlerin birbirleriyle, çalışanlarla ve yöneticilerle gerek zamanlı olarak bağlantı kurabilmesi sayesinde kontrollerin etkinliğinin, işletme politikalarına ve zorunlu düzenlemelere uygunluğunun ve iş süreçlerinin işletme amaçları doğrultusunda yürütüldüğünün sürekli izlenmesi sağlanabilir.
- İşletme faaliyetlerine veya olaylara gerçekleştikleri anda ya da en azından mümkün olan en yakın zamanda güvence sağlanmasını tanımlayan sürekli denetim, Endüstri 4.0 unsurlarının keşfedilmesiyle gerçek anlamda mümkün hale gelmiştir. Ancak Nesnelerin İnterneti ve üzerlerinde sensörler, kameralar, radyo frekansı ile tanımlama (RFID) cihazları, küresel konumlandırma sistemleri (GPS) taşıyan robotlar veya diğer siber fiziksel araçlar, gerçek zamanlı verinin elde edilebilmesini sağlayabilir. Denetimin kapsamına giren işlemler sonucunda üretilen ve ileri teknolojik araçlarla elde edilen daha çok yapılandırılmamış çeşitlilikte verinin çok kısa sürede analiz edilmesi, ancak Büyük Veri Analitiği olarak tanımlanan istatistiksel modelleme, veri madenciliği ve makine öğrenme gibi ileri matematiksel ve istatistiksel çözümlerle mümkün olmuştur.
- İşletme yöneticileri, Büyük Veri Analitiği araçlarının keşfedilmesiyle daha önce karar alma süreçlerinde göz ardı edilen farklı özelliklere sahip veriyi kullanabileceklerinin farkına varmışlardır. İşletmeler, Büyük Veri olarak tanımlanan ileri özelliklere sahip veriyi, Büyük Veri Analitiği araçlarıyla işleyerek, faaliyetleri için büyük fayda yaratan öngörüye ulaşabileceklerini keşfetmişlerdir.

- Bulut teknolojilerin, yüksek miktarda veriyi çok düşük maliyetle depolayabilmesi ve kesintisiz internet erişimiyle her an sunabilmesi, daha fazla verinin işlenebilmesinin önündeki engelleri kaldırmıştır. İşletme faaliyetleri sırasında tutulan log dosyalarından (günlük dosyalar) işletmenin faaliyet gösterdiği sektöre özgü ölçümlere kadar birçok veri, kontrol tehditlerinin ortaya çıkarılması ve daha etkin kontrollerin kurulması amacıyla kullanılabilecektir. Diğer taraftan özellikle siber tehditler ve güvenlik sorunları, Endüstri 4.0 unsurlarıyla değişen iç ve dış işletme çevresine daha iyi cevap verebilen kontrollerin geliştirilmesini bir zorunluluk haline getirmiştir.
- Endüstri 4.0 unsurlarının keşfedilmesi, sürekli denetimin temel bileşenlerinden biri olan sürekli risk değerlemenin gerçek anlamda mümkün olmasını sağlamıştır. Sürekli risk değerleme, risk seviyesi değişen işletme iç ve dış şartları dikkate alınarak öngörülen risk iştahının üzerine çıkan sistem ve süreçlerin üst yönetim tarafından gerçek zamanlı olarak tespit edilmesini sağlayacaktır. Büyük Veri Analitiğiyle zenginleşen teknoloji tabanlı denetim teknikleri, sürekli izleme araçlarına evrilen diğer Endüstri 4.0 unsurlarıyla gerçek zamanlı olarak tespit edilen değişimlere anlık olarak ya da en kısa zamanda tepki geliştirilmesinde güvence çalışanlarının karar süreçlerini destekleyecektir. Ayrıca yapay zekâ ve makine öğrenme, risk değerleme faaliyetlerinden ve olaylardan çıkarımlar yaparak, tepki geliştirme süreçlerinin otomatikleştirebilmesini ve insan düşüncesini taklit ederek tepki geliştirilmesini sağlama potansiyeline sahiptir.

Günümüz işletme dünyasında mikro ölçekli işletmeler bile, faaliyetlerinde teknolojik araçlardan yoğun bir şekilde yararlanmaktadır. Endüstri 4.0 veya başka bir ifadeyle 4. Sanayi Devrimi sonrasında işletme büyüklüğü veya faaliyet gösterdiği sektör fark etmeksizin birçok işletme, faaliyetlerini teknoloji ortamına taşımanın bir zorunluluk haline geldiğini kabul etmiştir. İşletme yöneticileri mümkün olan tüm işletme faaliyetlerinde dijital dönüşümü gerçekleştirmek amacıyla bilgi teknolojileri yatırımlarına büyük bütçeler ayırmaktadır. Birçok birim yöneticisi, mesailerinin büyük bir bölümünü faaliyetlerine tartışılmaz faydalar sunan teknoloji çözümlerini anlamaya çalışmaya veya faaliyetlerini dijital ortama nasıl taşıyabileceklerini tartışmaya ayırmaktadır.

Yönetişim, risk yönetimi ve uygunluk kavramlarının ilişkili olduğu performans yönetimi, güvence ve denetim, insan sermayesi ve kültür, iç kontrol, kalite yönetimi ve

stratejik yönetim gibi birçok alanı kapsayan YRU Çerçeveleri, söz konusu alanların teknolojik dönüşümünde üst yöneticilere, güvence çalışanlarına ve birim yöneticilerine yol gösterecektir. YRU çerçeveleri bütüncül bakış açılarıyla, üst yönetim, risk ve kontrol çalışanları ve iç denetçiler tarafından işletme faaliyetlerinde, güvence sağlama çalışmalarında ve risk değerleme süreçlerinde siber fiziksel araçlar, otonom robotlar ve nesnelerin interneti gibi unsurlardan nasıl daha fazla faydalanılabileceğinin keşfedilmesi ve uygulamaların işbirliği içinde tasarlanması için eşsiz çözümler sunacaktır.

Büyük Veri Analitiğinin daha fazla veriyi analiz edebilme gücü, birçok durumda örnekleme yapmak yerine evrenin tamamının incelenmesini sağlamıştır. Böylece daha güçlü örüntüler keşfedilebilir ve çıkarımlar yapılabilir. Endüstri 4.0 çağında iç denetçiler için örnekleme hatası tehlike olmaktan çıkmıştır. İç denetçilerin ve diğer güvence çalışanlarının karşı karşıya kaldıkları güncel sorun, belirsizliği artıran yapılandırılmamış verinin evrenin sınırlarının doğru belirlenmesini zorlaştırmasıdır. Faaliyetiyle ilgili verilerin tespit edilerek ilgisiz verinin kapsam dışında tutulması, uğraşmak zorunda oldukları verinin çeşitliliği ve hacmi devasa boyutlara ulaşan güvence çalışanları için karar alma süreçlerini ve mesleki yargıyı etkileyen önemli bir problemdir (Brown-Liburd, 2015). YRU yazılımları risk değerleme, kontrol ve güvence çalışmaları için gerekli olan tutarlı bilgiyi sunan teknolojik altyapıyı oluşturur. YRU yazılımları, güvence çalışanlarının aralarında düzen, uyum ve birliktelik olan güvence faaliyetlerinin ortak bir evrenden planlı, koordine ve işbirliği halinde yürütülmesi gerektiğini savunan YRU yaklaşımının teknolojik altyapısıdır. İşletmelerin spesifik sorunlarına çözüm arayan teknolojiler üzerinde çalışan YRU yazılımlarının sağladığı terminoloji ve işbirliği, ilgili işletme verisinden yaratılan ortak güvence evreni sayesinde, çalışanların ve yöneticilerin karar süreçlerini etkileyen ilgisiz veri sorununun büyük ölçüde çözümüne katkı sağlar.

Sürekli denetimin unsurlarından biri olan sürekli risk izleme ve değerlendirme faaliyetleri, işletme süreçlerinde iç ve dış şartlardan etkilenen risklerin değişiminin Endüstri 4.0 unsurlarıyla sürekli olarak izlenmesi ve elde edilen verilerin Büyük Veri Analitiği olarak tanımlanan ileri matematiksel ve istatistiksel tekniklerle değerlendirilmesini gerektirir. Sürekli risk değerlendirme faaliyetlerinde risk çalışanlarının öngörü ve çıkarımlar yaparak işletmenin risk yaklaşımını değişen şartlara göre yönlendirmesi hatta makine öğrenme ya da yapay zekâ teknolojileriyle çalışan otomatik kontrollerin geliştirilmesi, işletme amaçlarına yönelik düzenlenmiş risklerin bütüncül bir görünümünü sağlayan YRU yazılımlarıyla koordine edilebilir. YRU

yazılımları, işletmede herkesin üzerinde uzlaştığı doğrulanabilir veriye ulaşılmasını mümkün kılar.

Diğer taraftan işletmede verinin doğruluğunu sağlamak amacıyla özellikle güvence fonksiyonuyla ilişkili olan yedekleme ve geri yükleme, veri kurtarma, depolama, veri güvenliği ve erişim kontrolü gibi alanlarda BT denetimi süreçleri kritik öneme sahiptir. Otomatik kontrollerin ve BT denetiminin etkinliği, işletmede teknolojik araçlarla uyumlu çalışan, ortak terminoloji ve işbirliği sayesinde tüm işletme fonksiyonları için bilginin tutarlı bir şeklinin oluşturulmasını sağlayan yaklaşım ve bu yaklaşımın teknolojik altyapısı niteliğinde olan YRU yazılımlarıyla çok daha kolay hale getirilir.

### 3.12. YRU ve İç Denetim

Modern bir işletmede çok sayıda güvence çalışanının gerçekleştirdiği faaliyetlerin aynı mercekten bakılarak görülebileceği ve yönetilebileceği düşüncesi, işletme içinde farklı işler yürüten çalışanlar için oldukça radikal bir düşüncedir. Birçok kişiye göre bu fayda, YRU yaklaşımının en önemli vaatlerinden birisidir. Bu perspektiften bakıldığında, teknoloji sağlayıcıları, akademisyenler, uygulayıcılar ve kar amacı gütmeyen kurumlar tarafından yapılan farklı tanımları olmasına rağmen aslında daha basit düşünülürse YRU yaklaşımı, güvence ve iş performansının stratejik yönetiminden başka bir şey değildir. Bu sebeple, iç denetçilerin işletmeleri içinde rolünü büyük ölçüde değiştirme ve zenginleştirme potansiyeline sahiptir (Adams vd., 2016, s. 5).

Daha önce de ifade ettiğimiz gibi, YRU'nun getirdiği yaklaşım söz konusu faaliyetlerin (risk yönetimi, yönetişim, uygunluk, insan kaynakları, üretim, stratejik planlama vb.) birleştirilmesini değil bütünleştirilmesini ifade etmektedir. Aynı şekilde, YRU yaklaşımı güvence gruplarının ve faaliyetlerinin birleştirilmesini savunmaz. Bu anlamda kastedilen şey, YRU'yu oluşturan çeşitli disiplinlerde uygulayıcılar arasında ilişkilerin ve bağlantıların olduğudur. YRU yaklaşımının faydası bu bağlantıları kullanma becerisinin altında yatar. İşletmede bu bağlantıların ortaya çıkarılmasında en büyük sorumluluk iç denetçilere düşmektedir. İç denetçilerin YRU konusundaki sorumlulukları ana hatlarıyla şöyle sıralanabilir (Adams vd., 2016, s. 44):

- YRU sistemlerinin tasarımı konusunda danışmanlık faaliyeti yürütmek.
- Yönetişim, risk yönetimi ve uygunluk faaliyetlerinin sonuçlarının ölçülebilir olmasını sağlamak. (Bunu yapmak için çeşitli bileşenlerin nasıl bütünleştirildiğini ve uyumlaştırıldığını kavramak gerekir.)

- Risk ve kontrollere ilişkin ölçü birimlerinin seçilmesinde danışmanlık yapmak.
- Riskleri performans üzerindeki etkilerine göre sıralamak. (Performansı ölçme yöntemleri risk düzeyini nasıl etkiliyor? Riskler birbirleriyle ilişkili midir? Sorularına cevap aramak.)
- Kontrollerin oluşturulmasına danışmanlık yapmak.
- İstenen işletme başarısına ulaşmak için özel kontroller belirlemek. (Bu tür kontroller en düşük maliyetle nasıl uygulanabilir? Performans üzerindeki etkileri göz önüne alındığında hangi kontroller gereksizdir veya maliyet etkin değildir?)
- YRU teknolojileri ve örgütsel sertifikasyonların edinilmesi konusundaki çalışmaları desteklemek.
- YRU sisteminin tasarımının ve işleyişinin etkinliğini düzenli olarak gözden geçirmek. (Bu çalışma geleneksel iç kontrol değerlendirmesine benzemekle beraber YRU sistemi veya onun bileşenlerinden biriyle yapılan değerlendirme daha ayrıntılıdır.)

### 3.12.1. YRU Yaklaşımında iç denetimin sorumlulukları

İç denetim, organizasyonun risk yönetimi, yönetişim ve kontrol süreçlerinin etkinliğini değerlendirmek ve geliştirmek için sistematik ve disiplinli bir yaklaşım getirerek amaçlarına ulaşmasına yardımcı olur (IIA, 2010a, s. 2). IIA tarafından hazırlanan ve uygulanan iç denetim tanımı ve standartlar, hem YRU yaklaşımının geliştirilmesinde hem de en iyi şekilde değerlendirilmesinde (danışmanlık hizmeti ve güvence verme) iç denetçiye sorumluluk yükler (Mahzan & Yan, 2014, s. 160).

Hızla değişen ve karmaşıklığı giderek artan zorunlu ya da zorunlu olmayan düzenlemelerle dolu işletme çevresi, öncelikli olarak faaliyetler üzerinde önlem almaya odaklanan iç denetimin rolünü, sadece raporlama problemlerinin çözülmesine değil, aynı zamanda işletme performansının geliştirilmesine destek sağlama konusunda önemli bir etkiye sahip olan proaktif bir role dönüştürmüştür. Tartışmasız bir şekilde, günümüzün iç denetim fonksiyonu risk yönetimi, uygunluk, kontrol ve yönetişim (YRU) süreçlerinin performans verimliliğinin yanında bunların birbirleriyle uyumuyla da ilgilenmelidir (Jefferson Wells, 2009, s. 2).

İç denetçiler, YRU hakkında güvence ve danışmanlık yapma konusunda en doğru taraftır. Çünkü iç denetim işletme çapında devam eden bir YRU programının geliştirilmesinde ve başarılı bir şekilde düzenlenmesinde temel rolü üstlenen benzersiz

bir pozisyona sahiptir (Mahzan & Yan, 2014, s. 156). İç denetçiler, YRU yaklaşımını güvence faaliyetlerinde verimliliği artıran ve daha güçlü işletme performansı sağlayan bir girişim olarak dikkate almak zorundadırlar. İşletme çapında geniş yetkileri olan iç denetçiler, özel olarak görevlendirilmeseler bile, YRU'nun gelişimini destekleyecek pozisyondadırlar (Adams vd., 2016, s. 11).

Her şeyin ötesinde iç denetim risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliği ve verimliliği hakkında üst yönetime ve yönetim kuruluna bağımsız bir değerlendirme sağlamak için gereken teknik yeterliliğe ve kurumsal bilgiye sahip olmalıdır. Dünya klasındaki bir iç denetim birimi, sadece bilgi sağlamaktan çok daha fazlasını yapar. İşletmelerin karşılaştıkları zorlukları, kavramları ve trendleri tanıma konusunda yönetime destek sağlamak için gereken bilgiyi analiz etme, sentezleme ve yorumlamayı da sağlar. Ayrıca yönetim, kontrol çevresinin etkinliği ve verimliliğinin değerlendirilmesi ve işletmenin kontrol çerçevesine uyum sağlamasında iç denetime güvenir. İç denetim doğru bir YRU programının kurulması için çaba göstermelidir. İç denetim (Jefferson Wells, 2009, s. 2);

- YRU çerçevesi üzerinde önerilerde bulunur.
- İşletme çapında risk yönetimi stratejisinin geliştirilmesine yardım eder.
- En iyi uygulama önerilerinde bulunur ve uygulamaya yardım eder.
- Sistem ve süreçler hakkında öneriler getirir.
- İç denetim planını kurumsal risk yönetimiyle uyumlu hale getirir.
- Uygun yetenek transferini sağlar.

İç denetçilerin yönetime tavsiyeler sunarken dikkate alması gereken belki de en önemli konu, iç denetimin YRU faaliyetleri geliştirilirken veya YRU yaklaşımının savunduğu iç kontroller ve risk yönetimi eylemleri oluşturulurken yönetsel sorumluluk üstlenmemesidir. Ayrıca işletme faaliyetlerini ve birimlerini YRU yaklaşımının savunduğu felsefeye uygun hale getirmeye çalışırken, iç denetim biriminin organizasyon şemasında bağımsızlığını savunacak bir konuma oturtulması gerekmektedir.

İç denetçiler geleneksel risk yönetiminin ötesinde bütünleşik ve proaktif YRU yetenekleri geliştirilmesi için organizasyonlarına rehberlik etme noktasında önemli rol oynarlar. Bu yüzden, bir şirket veya kuruluşun bütün birimleri düşünüldüğünde, YRU'nun etkinliğini değerlendirme konusunda iç denetimden daha iyi bir pozisyona sahip faaliyet yoktur. Yönetim kurulu ve üst yöneticiler, YRU hakkında bir girişimde

bulunduklarında iç denetçiler, riski göz önünde bulunduran ve daha fazla şeffaflık sunan bu sisteme güvence sağlama fırsatına sahip olacaklardır (IIA, 2010b, s. 3).

Önümüzdeki üç ila beş yıl içinde, iç denetim birimlerinin, organizasyonlarının YRU ile ilgili konularda yürüttüğü faaliyetleri değerlendirmeleri, yönetim kurulu ve üst yönetime görüşlerini sunmaları gerektiği öngörülmektedir. Bu bağlamda kendilerinden işletmelerinde YRU'yu keşfetmeleri, desteklemeleri, uygulanmasına danışmanlık yapmaları ve güvence vermeleri beklenen iç denetçiler, yeniliklere açık olmalıdırlar. Önümüzdeki yıllarda iç denetimin kapsamını değiştirecek ve faaliyetlerine yön verecek YRU ile ilişkili öncelikler şunlardır (Swanson, 2010, s. 42-43):

*Kurumsal Risk Yönetimi (KRY) Programı*: Kurumsal Risk Yönetimi, yönetişim ve organizasyonel sonuçları geliştirmek için gümüş bir kurşun gibidir, çünkü anahtar amaçları belirler ve etkili yönetişimi sağlayan bu amaçlarla birlikte ortaya çıkan riskleri yönetir. İşletmeniz ister ISO31000'nin, ister COSO Treadway Komisyonunun risk yönetimi çerçevesinin, ister Açık Uygunluk ve Etik Grubu'nun (OCEG) yönetişim, risk ve uygunluk (YRU) yetenek modelinin ya da başka bir standardın savunucusu olsun; işletmeniz için KRY'nin hatta daha ileri seviyede risk yönetiminin geliştirilmesinin ve bu alanda destek alınmasının zamanı gelmiştir. İşletmenin KRY faaliyetlerinde iç denetimin yürütülmesi, işletme içindeki herkese risk yönetimindeki boşlukları ortaya çıkaran bir temel değerlendirme raporu sağlayacaktır.

*Genel Yönetişim Sistemi*: Yönetişim; kurumsal yönetişim, organizasyonel yönetim, iyi yönetişim, yönetişim risk ve uygunluk (YRU) gibi birçok farklı şekilde isimlendirilir. İç denetim, işletmenin yönetişim, risk yönetimi ve kontrol süreçlerine ilişkin üst yönetime ve yönetim kuruluna güvence sağlar. Bu yüzden, temel olarak, işletmenin çabalarını tanımlamak için kullandığı kavram hangisi olursa olsun iç denetim, genel yönetişim sistemine ilişkin bir fikir geliştirmeli ve sunmalıdır. Ayrıca, yönetişim yapısı içerisindeki sürdürülebilir kalkınma ve kurumsal sosyal sorumluluk sorunları da soruşturulmalıdır.

*Uygunluk ve Etik Programı Girişimleri*: Son beş yılda Uygunluk ve Etikle ilgili gelişmeler yüksek düzeyde ilgiyi ve yüksek miktarlarda fonu üzerine çekmiştir ve önümüzdeki beş yıl boyunca da çekmeye devam edecektir. İç denetim biriminin geçmişteki çalışmalarına bağlı olarak, uygunluk ve etik programlarının denetiminde, hem özel fırsatlar için ayrıntıya inilmeli hem de genel değerlendirmeler sağlanmalıdır.

### 3.12.2. YRU Yaklaşımının geliştirilmesinde iç denetim

YRU yaklaşımının geliştirilmesinde işletme içinde belki de üzerine en fazla sorumluluk düşen çalışanlar iç denetçilerdir. İç denetçiler, YRU yaklaşımı geliştirilmeden önce iç denetim birimlerinin bu sorumluluğu üstlenebilecek durumda olup olmadığını ve iç denetim fonksiyonunun nasıl etkilenebileceğini anlamalıdırlar. İç denetim yöneticileri için dikkate alınması uygun olan sorular şunlardır (Adams vd., 2016, s. 48):

- Hangi hizmetler sunulmaktadır?
- İç denetim ekibinin yapısı, becerileri ve yeterlilik seviyesi ne durumdadır?
- İç denetim faaliyeti işletme içinde ne derecede yetenek geliştirici bir fonksiyon olarak görülmektedir?
- İç denetim süreçleri ne kadar profesyonel ve metodolojiktir?
- İç denetim faaliyeti ne kadar niteliklidir ve iç denetimin kalitesi nasıl ölçülmektedir?
- İç denetimin işletme içinde ve kurumsal yönetim şemasındaki konumu nasıldır?
- İç denetim ne kadar bağımsızdır?

YRU süreçleri geliştirilirken, iç denetçiler, üst yönetime danışmanlık ve güvence verme işlevleri ölçüsünde sorumluluk üstlenirler. Frigo & Anderson tarafından (2009b) stratejik olarak YRU'nun tasarlanmasını ve uygulanmasını gösteren on adımlı bir yaklaşım, iç denetçilerin sorumlulukları da gözetilerek hazırlanmıştır. Bu adımlar YRU fonksiyonlarının öğrenilmesi ve kurulması için bir temel sağlar ve diğer işletme çalışanlarıyla birlikte özellikle iç denetçilere yol gösterebilir (Frigo & Anderson, 2009b, s. 34):

1. YRU fonksiyonlarını koordine etme. Yönetim, girişime katılması gereken risk ve güvence fonksiyonlarını belirleyerek ve çalışma takımını oluşturarak işe başlamalıdır. Bu fonksiyonların birçoğu hali hazırda bilinmesine karşın, yine de seçim süreci büyük bir dikkatle yürütülmelidir. İç denetçiler, kurumsal çapta bakış açılarıyla hareket ederek, işletmenin içerisinde faaliyet alanlarını belirlemeye yardım edebilirler.
2. Üst yönetim ve yönetim kuruluyla tartışma. Çalışma grubu tarafından geliştirilen ilk vizyon ve amaçlar üst yönetim, yönetim kurulu veya denetim komitesi tarafından açıkça ifade edilmeli ve tartışılmalıdır. Bu diyalog, girişimin hem faydalarını hem de önündeki engelleri içeren bir görüşmeyi içermelidir. Stratejik YRU çerçevesi bütün tarafların anlamasını sağlamak ve tartışmaları kolaylaştırmak

için kullanılabilir. Uygulamanın bu aşaması da iç denetime üst yönetim ve yönetim kurulu üyelerine stratejik bir danışman olarak hizmet etmek için önemli bir fırsat sunar.

3. İlk fırsatları belirleme. Çalışma grubu, uygulama için ilk fırsatların ortaya çıkabileceği alanları belirlemeye odaklanmalıdır. İşletmeler genellikle iletişimin, bilgi paylaşımının, iş programları yapmanın ve risk değerlendirmenin dahil olduğu süreçleri inceleyerek başlarlar. İletişim faaliyetleri incelendiğinde, birçok organizasyonun izleme ve raporlama sorunları için ortak ölçütler geliştirdikleri görülür. İşletmeler denetim programlarının ve fonksiyonların incelenmesinin koordinasyonunu ve paylaşılmasını da geliştirirler. Ayrıca risk ve güvence fonksiyonları arasında yürütülen risk değerlendirme yöntemlerinin çeşitliliği ve sayısı işletme maliyetleri üzerinde önemli bir unsur olabilir. Bu yüzden, risk değerlendirme faaliyetleri tutarlılığı sağlamak ve harcamaları azaltmak için verimli bir alan olabilir. Risk yönetimi incelenirken, işletmeler stratejik risk yönetimi gibi konuların geliştirilmesini ve bu alan için yetkinliklerin gerektiğinde elde edilmesini sağlayabilir.
4. İlk proje planını geliştirme. İlk fırsatların belirlenmesinin ardından detaylı planlar, başlayan projeleri geliştirmek için düzenlenmelidir. Özellikle ihtiyaçlar dikkatlice düşünülmelidir. İşletmeler, geleneksel olmayan atamalar için uygun kişileri takım çalışanı olarak kaydetmeyi düşünmelidir. Diğer taraftan, plan proje takımı için yetkin çalışanlara ve karşılaşılan engelleri öğrenmek için bir geri dönüt mekanizmasına sahip olunmalıdır.

İç denetçiler bu ilk projelerde önemli bir rol oynayabilirler. Uzmanlıklardan ve bilgi birikimlerinden nasıl yararlanılabileceğini veya eğer gerekirse, YRU girişimine tamamen katılmayı dikkatlice değerlendirmelidirler. Örneğin, sahip oldukları işletme çapında bakış açısıyla iç denetçiler, izleme gibi birbiriyle çakışabilecek sorunlu konuları belirleme ve mantıklı hale getirme noktasında iyi bir pozisyona sahiptirler. Ayrıca, bu ilk projeleri üstlenmek için denetim komitesine bakış açısı kazandırabilirler.

5. Risk politikasını tasarlama. Bir işletmenin genel risk politikası YRU'nun önemli bir bileşenidir. Politika geliştirmeye akıllıca yaklaşılmalıdır ve uygun hukuki, teknik ve kurumsal yönetişim bakış açısını yansıtan doğru çalışan ihtiyacı düşünülmelidir. Bazı işletmeler için var olan politikalar basitçe gözden geçirilmeli

veya güncellenmelidir. Diğerleri için ise yüksek seviyede görünürlüğü ve tartışma ortamını amaçlayan yeni politikaların yaratılması gerekecektir.

İç denetçiler politika geliştirme sürecine katkı sağlayabilir ve sürece dahil olan çalışanların eğitim almalarına yardımcı olabilir. Örneğin, işletmeye bağlı olarak, bazı eğitimler yönetim kurulu üyelerinin gelişen alanlardaki riskleri ve risk yönetimini anlamalarına yardımcı olabilir.

6. İlk proje planını yürütme. Etkili bir proje yönetimi süreciyle, ölçülen değerler ve başarı faktörleri tanımlanmalı ve geliştirilmesi gereken süreçler yürütülmelidir. Bu aşama, çalışanlar tarafından kavranan konuların anlaşılması için plan geliştirme süresince yaratılan geri dönüt mekanizmasını uygulamayı kapsamalıdır.
7. Vizyonu ve proje planını gözden geçirme. Bu noktada, çalışma grubu pratik deneyimleri kazanmalı ve başlangıç projelerinden sonuçları elde etmelidir. Çalışma grubu bu deneyimlere dayanan yaklaşımı, amaçları ve vizyonu yeniden gözden geçirmelidir. Bu süreç, çalışma grubunun nihai vizyonu ortaya çıkarmasını ve işletme için uygun amaçların geliştirilmesini mümkün kılar. Dikkat, sürekli gelişme için devam eden süreçlerin üzerinde olmalıdır, böylece pratikler zamanla geliştirilebilecektir. Son olarak, nihai vizyon ve amaçlar risk ve güvence fonksiyonları ve anahtar paydaşlar tarafından onaylanmalıdır.
8. Yönetim kurulu risk politikasını sonuçlandırma. İşletme bu aşamada, çalışma grubunun yeniden değerlendirmelerinden elde edilen çıktıları kullanarak vizyon ve amaçlarını kapsayan yönetim kurulu risk politikasını nihai haline getirmelidir. Çalışma grubunun ilk projenin sonuçlarından öğrendiklerine bağlı olarak bu süreç, politikanın basitçe onaylanmasını ya da çok daha sağlam bir biçimde yeniden belirlenmesini gerektirebilir.
9. Risk politikasını ve YRU yapısını onaylama. Yönetim kurulu ya da denetim komitesi tarafından biçimsel bir onaylama gerekecektir. İç denetçiler, bu aşama süresince, yöneticiler YRU yapısının hem tasarımında hem de uygulanmasında kendilerinden destek istediklerinde, yine uzmanlıklarını gösterme fırsatına sahip olurlar. İç denetçiler, birim yöneticileri ve üst yönetim arasında etkileşimi yönlendirerek, sadece çalışmaları geliştirmezler, aynı zamanda işletme içinde kendi itibarlarını ve önemlerini de artıracaklardır.
10. Nihai proje planını uygulama. Nihai plan tamamlandığında ve risk politikası ve yapısı onaylandığında, işletme, geliştirilen vizyonun başarılması ve planın

uygulanması için uygun bir pozisyon elde etmiş olmalıdır. Bu aşamada artık ihtiyaçlar daha iyi anlaşılmış olmalıdır ve genel başarı çıtasıyla ilişkilendirilmelidir.

İç denetçiler YRU süreçlerinde çift yönlü bir rol oynarlar. Bir yönüyle iç denetçiler pratikler hakkında diğer birimlere ve yönetime tavsiyelerde bulunurlar ve aynı zamanda YRU katılımcılarıdırlar. Diğer yönüyle, iç denetçiler, işletmenin yönetişim, risk yönetimi ve kontrol faaliyetlerinin etkinliği üzerinde güvence sağlamaktan da sorumludurlar. İç denetçiler, bu çift yönlü rolü birimlerinin özel statüsüne bağlı olarak yönetirler. Bazı durumlarda, iç denetim bir YRU projesinin başlatılmasında ve faydalarının işletme tarafından anlaşılmasında destek sunan bir rol üstlenir. Diğer taraftan farklı risk ve kontrol birimleri bu rolü üstlenirken, iç denetim, hem işletme birimlerine hem de üst yönetime tavsiyeler sunarak nesnel bir ses olur. İki farklı senaryoda da iç denetim risk ve kontrol çevresinin genel olarak bütünlüğünün korunmasına ve işletmenin YRU yaklaşımının değerinin farkına varmasına destek olur. İç denetimin tavsiyeleri, özellikle işletme içindeki bütün kesimler tarafından YRU yaklaşımının ne olduğunun açık bir şekilde anlaşıldığından emin olunması için önemlidir. Ayrıca iç denetim tarafından amaçların açıkça ifade edilmesi, YRU girişiminin başarıya ulaşması açısından çok önemlidir. İç denetim, odak noktasına amaçların ve stratejilerin oturtulması ve genel süreçlerde bütünlüğün sağlanmasında yüksek düzeyde etkili olabilir (Frigo & Anderson, 2009b, s. 36).

YRU yaklaşımının işletmede oturtulmasını sağlamak amacıyla geleneksel iç denetçilerin üzerlerindeki sorumluluğu gerektiği gibi yerine getirebilmeleri için bir takım bilgi ve becerileri öğrenmeye çalışmaları ve kendilerini bu girişime hazırlamaları gerekir. YRU girişimine liderlik etme konusunda iç denetçilerin kazanması gereken bilgi ve beceriler şöyle sıralanabilir (Adams vd., 2016, s. 19):

***YRU Yaklaşımını Stratejik Olarak Uygulamaya Geçirme Becerileri***: Önemli değişiklikler içeren girişimler, değişim yönetimi konusunda yöneticilik becerileri ve deneyime sahip olunmasını gerektirir. YRU yaklaşımının uygulamaya geçirilmesi basit bir projenin uygulanmasından çok daha köklü bir değişimdir ve iç denetçiler bu değişimi anlayacak, uygulayacak ve işletme içinde uygulanmasını sağlayacak yöneticilik yeteneğini kazanmalıdırlar.

***Risk ve Kontrol Çerçevelerinin Anlaşılması***: YRU; kurumsal yönetişim, risk yönetimi, iç kontrol, sürdürülebilirlik gibi kapsadığı alanlarda bu alanlara özel çerçevelerin kullanılmasına engel oluşturmaz hatta bunların kullanılması, YRU başarısını

artırabilir. İç denetçiler, COSO çerçevesi hakkında bilgi sahibi olabilirler ancak birbirinden çok farklı alanlarda ve bazen de birbiriyle çelişen çerçeveler vardır. İç denetçiler uygulanması amaçlanan bu çerçeveleri keşfetmeli ve anlamalıdırlar.

***Sektöre Yönelik Uygunluk ve Kurumsal Yönetişim Gereklilikleri Konusunda Uzmanlaşma***: İç denetim, kurumsal yönetimin köşe taşlarından birisidir ve uygunluk bir iç denetim türü olarak denetçilerin yoğun mesai harcadığı bir alandır. İç denetçiler, kendi faaliyet alanlarındaki işletme içi ve dışı uygunluk ve kurumsal yönetişim gereklilikleri konusunda bilgi sahibi olmalıdırlar.

***YRU Teknoloji Bilgisi***: YRU teknolojilerinin sayısı giderek artmaktadır. Birçok iç denetim faaliyeti çalışma kâğıtlarını, kendi amaçlarına yönelik olarak denetim planlarını ve programlarını otomasyon üzerine alarak teknolojiyi başarılı bir şekilde adapte etmektedirler. Diğer birçok teknolojinin yanında, özellikle sürekli denetim gibi teknolojiler anlaşılmalı ve YRU yaklaşımının bir parçası olarak kullanılmalıdır.

### 3.12.3. İç denetimin YRU'ya makul güvence verme sorumluluğu

YRU yaklaşımı; stratejik yönü, hedefleri, planları ve öncelikleri belirleyen ortak bir yönetim süreçleri ve kontroller paketi tarafından etkinleştirilmelidir. Bütünleşik bir yaklaşımın uygulanması; iç denetimin, risk yönetiminin, insan kaynaklarının, finansın, iç kontrolün, muhasebenin, uygunluğun, BT'nin ve diğer paydaşların hep birlikte ortak bir amaç için çalışmasını sağlayacaktır. YRU yaklaşımı, tüm ilgili işletme bölümlerinin potansiyel riskleri ve bu riskleri yönetmek için gereken kontrolleri belirlemesini sağlayacaktır. YRU süreci; yönetimin yönlendirmelerinin, planlarının ve faaliyetlerinin uygun ve sorumlu bir şekilde yerine getirilmesini garanti eden bir gözetim fonksiyonu sağlar. İç denetimin bu sürece ilişkin değerlendirmesi, iç ve dış paydaşlar için gerekli olan güvenceyi sağlayacaktır ve işletmeye yasal ve yasal olmayan düzenlemelere uyum sağlamasında yardımcı olacaktır (Coderre, 2009, s. 97).

İşletme çapında kontroller düşüncesi yeni bir kavram değildir. 20 yıldan daha fazla bir zaman önce COSO, 1992'de iç kontrol çerçevesini çıkarmıştır. Risk yönetimi ve uygunluk kavramları da yeni değildir, fakat geçtiğimiz 15 yılda risk ve uygunluğa olan ilginin arttığı gözlenmektedir. Sarbanes-Oxley ve Basel 2 gibi yasal düzenlemeler, küresel çapta işletmeler üzerinde büyük etkiler yaratmıştır. Tek başına uygunluk maliyetleri bile sayıları giderek artan yasalar ve düzenlemeler ile sert bir biçimde artmıştır. Fakat artan maliyetlerin temel sebebi operasyonel verimsizliktir: uyum çabaları

genellikle birbirinden kopuk mantalite ve yaklaşımlar sebebiyle tekrarlarla sonuçlanmıştır. Bu durum, birçok işletmenin uygunluk ihtiyaçlarının ötesine geçmesine ve YRU bileşenlerini bütünleşik bir süreç olarak görmesine yol açmıştır. İç denetim, YRU'nun işletme çapında bir yaklaşım yoluyla ele alınmasını sağlamalıdır. Böylece iyi yönetişim ve risk yönetimi çerçevesinin sürekli olarak değerlendirilmesi ve yürürlükteki yasa ve düzenlemelere uyum gösterilmesi sağlanır.

İç denetim, genel amaçlara ulaşılacağı konusunda makul bir güvencenin olup olmadığını belirlemek için YRU bileşenlerinin bağımsız bir değerlendirmesini yürütür. Bunu yapmak için, iç denetçiler ortaya çıkan risk alanlarını, yönetimin izleme programlarının etkinliğini ve yönetimin tanımlanmış risklere tepkisinin yeterliliğini göz önünde bulundurmalıdır. İç denetçiler risk yönetimi, kontrol ve yönetişim süreçlerinin değerlendirilmesi için sistemli bir yaklaşım getirmelidirler. Ayrıca, yönetimin sorumluluklarını yerine getirme konusundaki performansını değerlendirmeleri gerekir. YRU süreçlerinin denetiminin amacı, bu süreçlerin istendiği gibi işlediğine ve işletmenin amaçlarına katkıda bulunacağına dair makul güvence sağlamaktır. Ayrıca, YRU bileşenlerinin iç denetimi, etkinlik ve verimliliği geliştirmek için yönetime uygulanabilir öneriler sunabilir.

Birincil bir görev olarak, iç denetim yeni yordamlar ve süreçler geliştirmek yerine YRU sürecinin mevcut çerçeveler ve süreçler üzerine kurulmasını sağlamak için uğraşmalıdır. İç denetçiler, denetimler sırasında veya yıllık riske dayalı denetim planını geliştirme sürecinin bir parçası olarak organizasyonun çeşitli alanlarındaki risk yönetimi uygulamalarını incelemiş olacaklardır. Var olan risk yönetimi süreçlerinin bilgisi; anahtar çalışanların, hali hazırda değerlendirilmekte olmayan veya birbirini tekrarlayan alanları belirlemesi için önemlidir. İç denetçiler, bu bilgiyi, YRU bileşenlerinin mevcut kurumsal yeterlikler, süreçler ve yapılarla uyumlu hale getirerek değişim direncini ve çaba tekrarını azaltmada yönetime yardımcı olmak için kullanabilirler.

Denetim incelemesi, YRU bileşenlerinin bütünleşme ve işbirliğini destekleyen ortak bir dil ve yaklaşımı kullanmasına destek sağlayabilir. Örneğin, tutarlı tanımlar işletme genelinde farklı risk türlerinin karşılaştırılmasına olanak tanır. Ayrıca iç denetim, süreçlerin bütünleşme ve tekrardan kaçınma seviyesini değerlendirebilir. Risk bilgisi, boşlukları ve tekrarları azaltmak için işletmenin bütün alanlarına iletilmeli ve onlarla paylaşılmalıdır. İç denetim, risk yönetimi faaliyetlerinin farkında olmalıdır. Risk faaliyetlerini denetim planlama döngüsü ile senkronize etmek, zamanında bilgi ve

analizle desteklenen daha hızlı ve riski göz önünde bulunduran kararlara destek sağlayabilir. Son olarak iç denetim, anahtar işletme süreçlerine ve yordamlarına, YRU faaliyetlerinin yerleştirilmesinin garanti edilmesine destek sağlayabilir. YRU yaklaşımı, zorunlu bir faaliyet ya da sadece uyum sağlanması gereken ek bir adım olmamalıdır. İç denetim, YRU yaklaşımının kurumsallaşma derecesini değerlendirebilir ve karar alma ile stratejik planlama süreçlerinin bir parçası olabilir (Coderre, 2009, s. 98).

Kapsamlı bir YRU denetimi, iç deneticilerin (1) yönetimin riski tanımlamak, değerlendirmek ve yönetmek için etkili bir sistemin tasarlanmasına ve yürütülmesine (2) iç kontrol sisteminin istenildiği gibi yeterliliğine ve düzgünce yürütüldüğüne (3) genel yönetişim sürecinin düzgün çalıştığına makul güvence sağlamalarına olanak sağlar. İç denetim yıllarca çeşitli isimler altında yönetişim, risk ve uygunluk süreçlerinin denetimini gerçekleştirirken, sadece son yıllarda söz konusu süreçleri ve yordamları bütünleştirmiştir. Eskiden söz konusu yönetim fonksiyonları, birbirinden kopuk bölümler halinde yürütülüyordu, bu durum iç denetimin söz konusu süreçlerin yeterli ve etkin olduğu hakkında makul güvence vermesini zorlaştırmıştır. Fakat YRU yaklaşımı, denetimin bir bağlantı noktası olmasını sağlamış ve denetim tavsiyelerini ele almak amacıyla yönetimin hesap verebilirliğini geliştirmiştir (Coderre, 2009, s. 98).

YRU faaliyetlerinin değerlendirilmesi, iç kontrolün ve risk yönetiminin incelenmesini kapsamalıdır. Denetimden sorumlu yönetici (CAE) risk yönetimi ve kontrol süreçlerinin etkinliğini değerlendirmek için yeterli olabilecek denetim faaliyetlerinin tamamından oluşan risk tabanlı bir denetim programı geliştirmelidir. Yıllık plan tüm anahtar işletme birimlerini ve işletme fonksiyonlarını kapsamalıdır. Planlanmış iç denetimler yürütülürken, risk yönetimi süreçleri değerlendirilmelidir. Son olarak, yıllık denetim planı, risk çevresindeki iç ve dış değişimlere cevap verebilmeyi sağlamak amacıyla sürekli olarak incelenmelidir ve gerekli görüldüğünde güncellenmelidir (Coderre, 2009, s. 99).

### 3.12.4. YRU süreçlerinde üç hatlı savunma modeli ve iç denetim

İşletme içinde risk yönetimi, iç kontrol, iç denetim, uygunluk gibi farklı güvence sağlayıcıları çok sayıda rapor üretirler. Ancak çoğu zaman raporlardan elde edilmesi beklenen fayda, doğru tartışma ortamlarına ulaşmadan kaybedilir. Birçok işletmede güvence faaliyetleri arasında koordinasyonun olmadığı bir yaklaşım, birbiriyle kısmen örtüşen ya da birbirinin kopyası çok sayıda güvence çalışmasına ve bu sebeple güvence kaynaklarının verimsiz kullanılmasına ya da güvence boşluklarına yol açar. Diğer taraftan bunun önüne geçmek amacıyla riskler üzerinde aşırı kontrollerin uygulanması güvence yorgunluğuna sebep olur. Bu sorunlardan kaçınmanın makul çözümü, işletmenin maruz kaldığı temel risklere karşı güvence faaliyetlerini bütünleştirmeyi düşünmektir. Bu fikir bütünleşik güvence olarak ifade edilir (Sarens vd., 2012, s. 22).

Bütünleşik güvence; denetim, risk yönetimi ve diğer güvence fonksiyonları arasında gerekli olan işbirliği ve koordinasyonun nasıl sağlanacağı ve özellikle iç denetimin bu kapsamda bağımsızlığını koruması için nasıl hareket etmesi gerektiğinin sınırları hakkında öneriler getirir. YRU yaklaşımı ise, özellikle güvence fonksiyonlarını kapsayacak şekilde işletmenin uygun faaliyetleri arasında koordinasyon ve işbirliği için çalışanların, stratejinin, iş süreçlerinin ve teknolojik altyapının uygun hale getirilmesini sağlar. YRU yaklaşımının geliştirilmesi ve BT ile desteklenmesi, işletmenin bütünleşik güvenceye ulaşmasının önündeki engelleri kaldırır.

YRU yaklaşımı risk yönetimi, denetim, uygunluk, iç kontrol gibi güvence faaliyetlerinde tüm güvence fonksiyonları ve çalışanları arasında tam bir koordinasyonun ve işbirliğinin sağlanması gerektiğini savunur. YRU yaklaşımına göre; işletmede stratejinin, süreçlerin, teknolojinin ve çalışanların uygun şekilde düzenlenmesiyle bütüncül bir bakış açısına ulaşılabilir. İşletme çalışanları arasında ortak hareket etme kültürünü ve ihtiyaç duyulan bütüncül görünümün elde edilmesi için çaba gösterilmesini savunan YRU yaklaşımı, güvence çalışanları arasında da aynı kültürün benimsenmesi, bütüncül görünümün elde edilmesi ve faaliyetlerde koordinasyonun sağlanması iddiasındadır. Böylece ortak paylaşılan güvence evreni oluşturulur ve güvence faaliyetlerinde gereksizliklerin ve boşlukların önüne geçilebilir yani bütünleşik güvence sağlanır. Bu bağlamda YRU yaklaşımı, bütünleşik güvence ile aynı amaçlara ulaşılmasını savunur.

Bütünleşik güvencenin sağlanması için tüm güvence sağlayıcıları arasında tam bir koordinasyonun sağlanması gereklidir. Tek hatlı bir savunma modeli, etkin risk

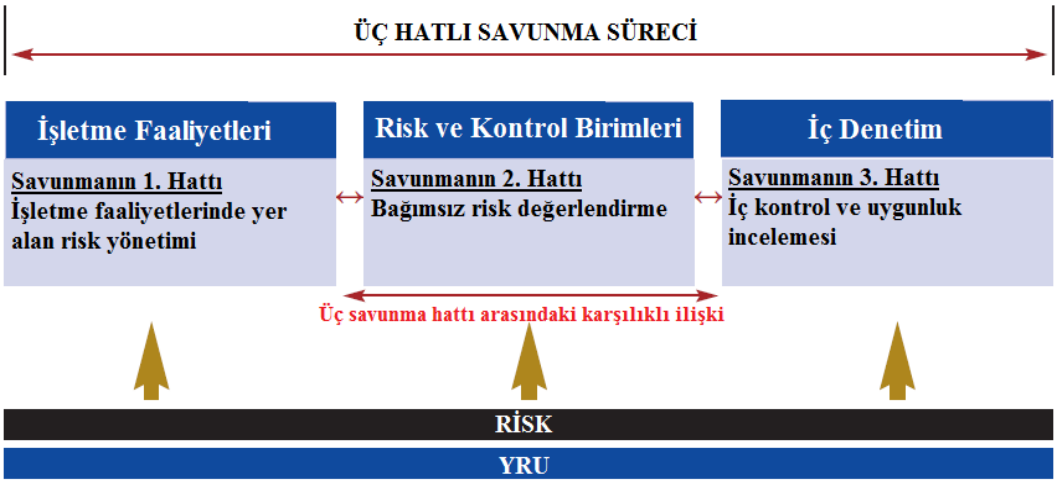
yönetimine ve iç kontrole güvence verilmesi için gereken koordinasyonu sağlayamaz. IIA tarafından bütünleşik güvencenin sağlanması için iç denetimin üçüncü savunma hattında bağımsız ve ayrı bir fonksiyon olarak konumlandırıldığı üç hatlı savunma modelinin, tüm güvence fonksiyonlarının koordinasyonu ve iç denetimin bağımsızlığı konusunda en doğru yaklaşım olduğu savunulmaktadır (Huibers, 2015, s. 2).

Hollanda Kamu Muhasebecileri Enstitüsünün (NIVRA) hem anket hem de yüz yüze görüşme yoluyla iç denetçilerin YRU yaklaşımının geliştirilmesindeki rolü ve YRU faaliyetlerinde etkili iç denetimin nasıl yapılacağının cevabını aradığı çalışmada; risk ve kontrol fonksiyonlarının oluşturulmasında, IIA'nın da pozisyon raporları aracılığıyla iç denetçilere önerdiği üç hatlı savunma modelinin olağanüstü etkili olduğunu vurgulamıştır (Man vd., 2010, s. 5).

#### *3.12.4.1 Üç hatlı savunma modelinde iç denetimin bağımsız konumu*

Üç hatlı savunma modeli, YRU ihtiyaçlarının karşılanmasına katkı sağlar. Her bir savunma hattı, işletme içinde koruma katmanı yaratarak risk yönetimini güçlendirir. Bu savunma katmanları arasındaki karşılıklı ilişki, YRU yaklaşımını ve bir işletmedeki olgunluk düzeyini anlamanın temelini oluşturur (Tadewald, 2014, s. 12). Şekil 3.22, Üç hatlı savunma sürecinde her bir hattın üstlenmesi gereken temel faaliyetlerin çerçevesini çizmektedir.

Üç hatlı savunma modeline göre, risk yönetimi çerçevesinde yönetim kontrolleri savunmanın birinci hattı, yönetim tarafından kurulan çeşitli risk, kontrol ve uygunluk gibi gözetim birimleri savunmanın ikinci hattı ve bağımsız güvence yani iç denetim üçüncü hattı oluşturur. Bu üç hattın her biri işletmenin genişleyen yönetişim çerçevesinde açık bir rol oynar (IIA, 2013, s. 2).




**Şekil 3.22.** *Üç Hatlı Savunma Modeli YRU İlişkisi (Tadewald, 2014, s. 3)*

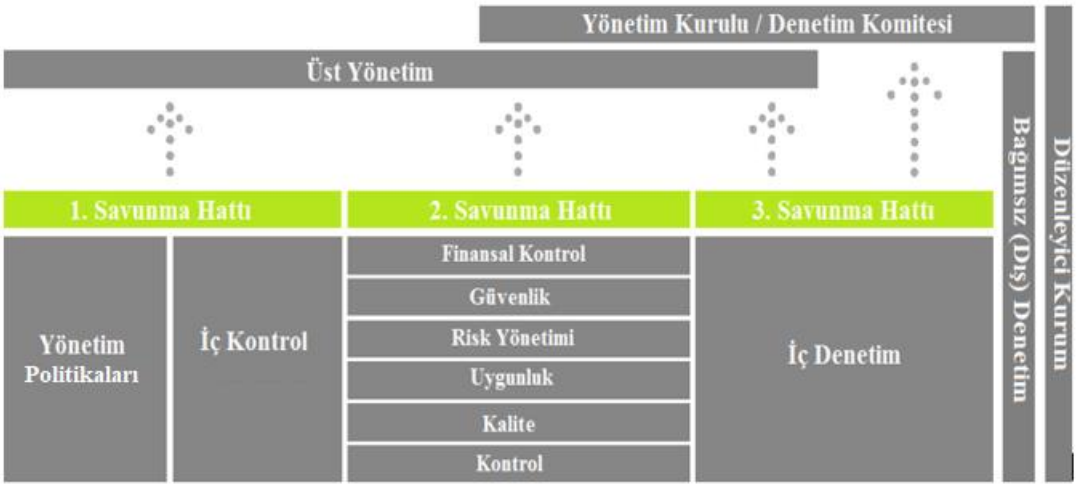
Hedeflere ulaşılıp ulaşılmadığından ve etkili kontrol önlemlerinin alınıp alınmadığından sorumlu yönetim hattı, savunmanın ilk hattıdır. İç denetim fonksiyonuna ek olarak birçok işletme risk yönetimi, uygunluk ve ayrı bir iç kontrol gibi diğer risk ve kontrol birimlerine sahiptir, bunlar savunmanın ikinci hattını oluşturur. Risk ve kontrol birimleri, kısmen politikaların geliştirilmesinden, uygulanan politikaların ölçülmesinden ve politikaların uygunluğunun izlenmesinden sorumludur. İç denetim birimi, işletmenin iç kontrol sisteminin bir parçasını oluşturan bu risk ve kontrol birimlerinin etkinliğini değerlendirir. Bu süreç boyunca, iç denetim birimi, bu birimlerdeki eksiklikleri veya gereksizlikleri belirler ve böylece birimlerin etkinliğini geliştirir. İç denetim birimi savunmanın üçüncü hattında yer alır ve bu pozisyonu gereği bağımsız olmalıdır (Man vd., 2010, s. 5).

Üç hatlı savunma modelinin amacı, risk yönetimi, kontrol ve güvence faaliyetlerinde, her fonksiyonun görev ve sorumluluklarına uygun şekilde koordinasyonu sağlamaktır. Bu faaliyetlerin işbirliği içinde yürütülmesi, işletmeye örgütsel yapının tüm seviyelerinde daha fazla şeffaflık ve operasyonel verimlilik gibi birçok fayda sağlar. Kopuklukları ortadan kaldırır. Farklı savunma hatları arasındaki koordinasyonu geliştirmek, işletmenin risk yönetimi çabalarında uyumu ve sinerjiyi sağladığı için çok değerlidir. Öte yandan, daha iyi bir koordinasyon, riskleri ele almak için güvence kaynaklarının kullanımı açısından da faydalıdır, çünkü birlikte çalışmadaki başarısızlık, işin çoğalmasıyla sonuçlanır, bu da maliyetli ve zaman alıcıdır. Bütünleşik güvencenin sağlanması işletmeye aşağıdaki faydaları sağlar (Sarens vd., 2012; Huibers, 2015):

- Daha iyi kararlar alınmasına yardımcı olur.

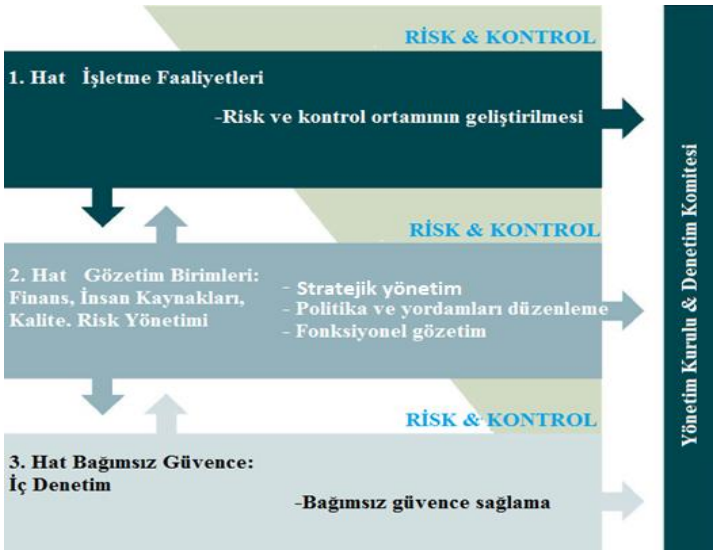
- İşletme için hangi faaliyetlerin öncelikli olduğunun belirlenmesine destek olur.
- Bütüncül risk görünümü sunar ve böylece yönetim kurulu ve üst yönetime risk yönetiminde kolaylık sağlar.
- Güvence fonksiyonları arasında tek bir ses ve taksonomi oluşturulmasına yardımcı olur.
- Yönetimin risk bilinci ve iş bilgisini artırır.
- Risk ve güvence faaliyetlerinde kopuklukların ortadan kaldırılmasına destek olur.
- İşletmelerde güvence ve risk faaliyetlerinin karmaşıklığını ortadan kaldırır ve yönetimini kolaylaştırır.
- Şeffaflık ve hesap verebilirlik seviyesini artırır.
- Bilginin daha verimli toplanmasını ve raporlanmasını sağlar.
- Güvence kaynaklarının daha iyi kullanımını teşvik eder.
- İç denetim faaliyetlerinin kalitesini artırır.
- Güvence faaliyetlerini standartlaştırır.
- Yönetişim, risk yönetimi ve kontrol faaliyetlerinin daha etkili izlenmesine destek sağlar.

Üç hattın her biri, işletmenin yönetişim çerçevesinde belirgin bir rol oynamaktadır. Her bir hat kendi rolünü yerine getirdiğinde, işletme genel amaçlarında başarıya ulaşabilecektir. Bir organizasyon içindeki herkes, iç kontrol için bir takım sorumluluklara sahiptir. Önemli görevlerin yerine getirildiğinden emin olmak için Üç Hatlı Savunma Modeli, belirli roller ve sorumluluklara açıklık getirir. Bir işletme, bu üç hattı düzgün şekilde yapılandırdığında ve etkili bir şekilde işlettiğinde, işletmenin söz konusu güvence faaliyetlerinin kapsadığı alanda bir boşluk olamaz, gereksiz bir çaba tekrar edilmez ve risk, kontrol ve güvence etkin bir şekilde yönetilir. Böylece YRU yaklaşımının temel amaçlarından biri olan gereksizliklerin ortadan kaldırılması sağlanmış olacaktır. Ayrıca üç hatlı savunma modeli sayesinde yönetim kurulu, işletmenin en önemli riskleri ve bu risklere yönetimin nasıl tepki vereceği hakkında eksiksiz bilgi alma fırsatına sahip olacaktır. Şekil 3.23 yönetim kurulu, üst yönetim, iç denetim, bağımsız denetim ve diğer güvence fonksiyonlarının üç hatlı savunma modelindeki konumunu göstermektedir.




**Şekil 3.23.** *Üç Hatlı Savunma Modelinde Roller (Chambers, 2014, s. 2)*

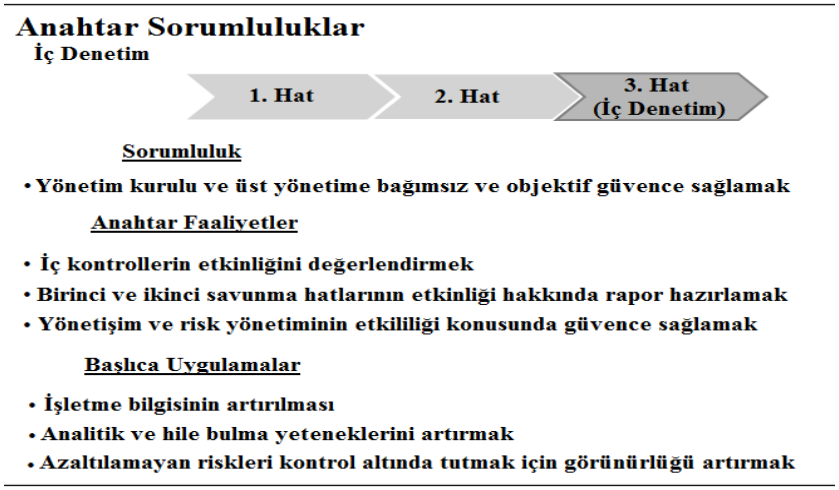
Savunma hatlarının her birindeki fonksiyonlar, işletmeden işletmeye göre değişebilir ve bazı fonksiyonlar savunma hatları boyunca birleştirilebilir veya bölünebilir. Bu durum işletmenin organizasyon şemasına bağlıdır. Örneğin bazı işletmelerde, ikinci hattaki uygunluk fonksiyonu ayrı bir birim olarak konumlanmak yerine ilk hattaki kontrollerin tasarım sürecinde yer alırken, ikinci hattaki diğer fonksiyonlar öncelikli olarak bu kontrollerin izlenmesine odaklanabilirler. Şekil 3.24, üç hatlı savunma modelinde risk ve kontrol sorumluluklarını göstermektedir. Modelde işletmenin üç savunma hattını nasıl yapılandırdığına bakılmaksızın uygulayabileceği, birkaç önemli ilke vardır (Anderson ve Eubanks, 2015, s. 3):




**Şekil 3.24.** *Üç Hatlı Savunma Modelinde Risk ve Kontrol (Lvov, 2009, s. 3)*

- İlk savunma hattı bir işletmenin amaçlarına ulaşmasını önleyebilecek ya da kolaylaştırabilecek, riskleri oluşturan ve/veya yöneten iş ve süreçlere sahiptir. Buna doğru riskleri alma dahildir. Birinci savunma hattı, bu risklere cevap vermek amacıyla işletmenin kontrollerinin tasarlanması ve yürütülmesini içinde barındırır.
- İkinci hat, risk ve kontrolün etkin bir şekilde yönetilmesini sağlamaya yardımcı olmak için uzmanlığa, süreç mükemmelliğine ve yönetimin izleme süreçlerine katkı sağlamak amacıyla ilk hattan sonra gelerek yönetimi desteklemek üzere yürürlüğe konmuştur. Savunma fonksiyonlarının ikinci hattı, ilk savunma hattından ayrı olmakla birlikte yine de üst yönetimin kontrolü ve yönetimindedir ve genellikle bazı yönetim fonksiyonlarını gerçekleştirir. İkinci hat, aslında risk yönetiminin birçok yönüne sahip olan bir yönetim ve/veya gözetim fonksiyonudur.
- Üçüncü hat, üst yönetim ve yönetim kuruluna hem ilk hem de ikinci hatların yönetim kurulu ve üst yönetimin beklentileri ile tutarlı çaba gösterilmesi konusunda güvence sağlar. Üçüncü savunma hattının, genellikle, nesnelliğini ve örgütsel bağımsızlığını korumak için yönetim işlevleri gerçekleştirmesine izin verilmemektedir. Buna ek olarak, yönetim kuruluna raporlama yapar. Bu nedenle üçüncü hat kendisini savunmanın ikinci hattından ayıran bir yönetim fonksiyonu değil, güvence fonksiyonudur.

İç denetim savunmanın üçüncü hattında yer alan konumuyla, diğer roller arasında yönetişim, risk yönetimi ve iç kontrolün etkinliği ve verimliliği ile ilgili güvence sağlamaktan sorumludur. İç denetim çalışmalarının kapsamı, bir işletmenin faaliyetlerinin bütün yönlerini içinde barındırır. İç denetimi diğer iki savunma hattından ayıran en temel unsur, örgütsel bağımsızlık ve objektiflik düzeyinin yüksek olmasıdır. Üç hatlı savunma modelinde iç denetimin anahtar sorumlulukları Şekil 3.25'te gösterilmiştir.




**Şekil 3.25.** *Üç Hatlı Savunma Modelinde Anahtar Sorumluluklar (Burns & Nordstrom, 2015, s. 5)*

İç kontrolü tasarlamak ve uygulamak, iç denetçilerin sorumluluklarından biri değildir ve iç denetçiler aslında işletme faaliyetlerinde sorumluluk üstlenmez. Birçok işletmede iç denetimin bağımsızlığı, CAE ve yönetim kurulu arasındaki doğrudan raporlama ilişkisiyle daha da güçlendirilmiştir. Bu yüksek örgütsel bağımsızlık sayesinde iç denetçiler, yönetişim, risk ve kontrol ile ilgili olarak yönetim kuruluna ve üst düzey yönetime güvenilir ve objektif bir güvence sağlama konusunda en uygun konumda bulunmaktadırlar. Yönetim kurulu ve üst yönetime raporlanan bu güvencenin kapsamı genellikle aşağıdakileri kapsar:

- Faaliyetlerin etkinliği ve verimliliği de dahil olmak üzere geniş bir amaç yelpazesi; varlıkların korunması; raporlama süreçlerinin doğruluk ve güvenilirliği; yasalar, yönetmelikler, politikalar, yordamlar ve sözleşmelere uyulması.
- İç kontrol ortamı; bir işletmenin risk yönetimi çerçevesinin tüm unsurları (risk belirleme, risk değerlendirme, riske cevap verme gibi.); bilgi, iletişim ve izlemeyi kapsayan risk yönetimi ve iç kontrol çerçevesinin tüm bileşenleri.
- Satış, üretim, pazarlama, güvenlik, ve müşteri ilişkileri gibi iş süreçlerini ve bunların yanında destekleyici fonksiyonları (bütçeleme, bordrolama, gelir ve gider hesapları, satın alma, varlık yönetimi, envanter, BT) kapsayacak şekilde genel olarak işletmenin tamamı, bölümleri, bağlı şirketler ve işletme birimleri.

Bütünleşik güvencenin sağlanması için iç denetimin diğer fonksiyonlarla koordinasyonu ve işbirliği gerekir. Yönetim açısından bakıldığında fonksiyonların bütünleşmesi, işletmenin YRU yapısının tasarımına temel teşkil edebilir. İşletmenin YRU süreçleri yeterli olgunluğa ulaşana kadar iç denetim, metodolojinin tasarımını destekleyen

geçici bir rol üstlenebilir. İşletmenin güvence modelinin bir parçası olarak bazı fonksiyonların bir araya getirilmesi doğru bir tercih olabilir. Fonksiyonların bütünleştirilmesi için kontrollerin kapsamı azaltılabilir. Denetim, yönetişim, risk, iç kontrol ve uygunluk tek bir şemsiye altında toplanarak verimlilik ve sinerji artırılabilir. Bu durum ikinci savunma hattında yer alan fonksiyonların, iç denetim fonksiyonu ile iç denetimin bağımsızlığını ve tarafsızlığını tehlikeye atmadan nasıl ve hangi seviyede bütünleştirileceği sorununu ortaya çıkarmıştır. Uluslararası Mesleki Uygulama Çerçevesinde, IIA pozisyon raporlarında ve rehberlerinde iç denetimin diğer fonksiyonlar ile bütünleşirken bağımsızlığını ve tarafsızlığını sağlamak için gerekli görülen temel koşullar ve önlemler Tablo 3.11'de sunulmuştur (Huibers, 2014, s. 25):

**Tablo 3.11.** *İç Denetimin Bağımsızlığını Koruyan Koşullar ve Önlemler (Huibers, 2014)*

| | |
|---|---|
| Verimlilik tehlikeye atılmamalıdır: Savunma hatları, iç denetimin bağımsızlığını ve nesnel güvence sağlama konusunda etkinliğini tehlikeye sokacak şekilde bütünleştirilmemeli veya koordine edilmemelidir. | IIA Pozisyon Raporu: Üç Hatlı Savunma (2013) |
| Sonuçlar netleştirilmelidir: İç Denetim, bütünleşmenin etkisini üst yönetime ve yönetim organlarına açıkça belirtmelidir ve onay alınmalıdır. | IIA Pozisyon Raporu: Üç Hatlı Savunma (2013) |
| Yönetim sorumluluğu üstlenilmemelidir: İç Denetim, denetlediği faaliyetler ve birimler ile ilgili herhangi bir yönetsel sorumluluk almamalıdır. | IIA Pozisyon Raporu: ERM (2004-2009) |
| Sorumluluklar açıklanmalıdır: Belirsizlikten kaçınmak ve organizasyonda netlik sağlamak için sorumluluklar denetim yönetmeliğinde açıklanmalıdır. | Nitelik Standardı 1000 |
| Denetim komitesinin onayı alınmalıdır: İç Denetim'in ikinci savunma hattı fonksiyonlarını veya metodolojinin tasarımını desteklediği geçici bir rolü söz konusu olduğunda denetim kurulunun onayı alınmalıdır. | Performans Standardı 2050 |
| Zorunlu hallerde dış kaynak kullanılmalıdır: İç denetimin ikinci savunma hattında bulunan faaliyetlere katılması durumunda, en azında bir süre, güvence dış kaynak kullanımıyla sağlanmalıdır. | Performans Standardı 2010/2050 |
| Görevler ayrılmalıdır: Olumsuz sonuçların ortaya çıkma potansiyeli olan işler, farklı kişilere ve/veya birimlere yaptırılmalıdır. | Performans Standardı 1130 |

### *3.12.4.2 Üç hatlı savunma modelinde iç denetimin YRU sorumlulukları*

IIA'nın pozisyon raporları yoluyla YRU faaliyetlerinin denetiminde iç denetçilere önerdiği üç hatlı savunma modelinde iç denetimin temel sorumlulukları güvence rolü, danışmanlık rolü, katılımcı rolü ve asla üstlenmemesi gereken sorumluluklar olarak dört başlıkta ele alınmaktadır. İç denetim işletmenin büyüklüğüne, faaliyet gösterdiği sektörün özelliklerine ve işletmeye özgü koşullara göre farklı sorumluluklar da üstlenebilmesine karşın genel olarak üstlenmesi gereken YRU sorumlulukları Tablo 3.12'de yer almaktadır (Huibers, 2014, s. 19).

**Tablo 3.12.** *Üç Hatlı Savunma Modelinde İç Denetimin YRU Sorumlulukları (Huibers, 2014)*

| | |
|---|---|
| **Güvence Rolü** | İşletmenin ikinci savunma hattında bulunan faaliyetlerin ve fonksiyonlarını etkinliğine güvence vermek (Örneğin risk yönetimi fonksiyonunun etkinliğini değerlendirmek)<br>Uygunluk ve süreç denetimi yaparak güvence vermek (Örneğin BT, insan kaynakları veya tedarik zinciri süreçlerinin faaliyet denetimini yapmak)<br>Üst yönetime, risk yönetimine ilişkin konsolide raporlar hazırlamak (Örneğin İç denetim esnasında uygunluk ile ilgili bir güvenlik incelemesinin raporla üst yönetime sunulması sürecinde riskleri tanımlamak)<br>Kontrol çerçevesini ve ilgili risk ve kontrolleri değerlendirmek (Örneğin bir iş sürecinin yeniden tasarımında kontrol çerçevesi üzerinde incelemeler geliştirmek |
| **Danışmanlık Rolü** | İkinci savunma hattındaki fonksiyonlara YRU'ya ilişkin tavsiyeler vermek (Örneğin Bir risk değerlendirme programının tasarımı konusunda tavsiyelerde bulunmak)<br>İç kontrolün tasarımı konusunda danışmanlık (Örneğin OCEG çerçevesine uygun kontrol eylem ve faaliyetlerinin tasarımına ilişkin tavsiyeler vermek)<br>Nesnel gözlemcilik yapmak (Örneğin Karşılaşılan zorluklara karşı en iyi uygulamalar konusunda organizasyona ve yönetime, yönetim sorumluluğu üstlenmeden yol göstermek)<br>Eğitimler vermek (Örneğin geliştirilen yordamlar ve kontroller konusunda eğitim desteği sunmak) |
| **Katılımcı Rolü** | İşletmenin risk değerlendirme süreçlerine destek olmak (Örneğin risk farkındalığı ve risk değerlendirme konusunda yönetime yardımcı olmak)<br>Yönetişimi, risk yönetimini ve kontrolleri geliştirmek amacıyla YRU girişimlerini başlatmak (Örneğin risk ve kontroller üzerinde yönetimi ve izlemeyi geliştiren projeler başlatmak)<br>Risk metodolojisi ve Kontrol Öz Değerlendirmeleri ile ilgili faaliyetleri koordine etmek (Örneğin Kontrollerin değerlendirilmesi sürecini destekleyerek işletme politikalarına uygunluğun değerlendirilmesini sağlamak)<br>Kontrollerin belgelendirilmesini sağlamak (Örneğin bir iş sürecinin yeniden tasarımında uygun belgelendirmenin yapılmasını sağlamak)<br>Riskleri tanımlamanın yanında gerçek iş konularında kalite güvence desteği sağlamak (Örneğin tanımlanan risklerin nasıl kontrol edileceği konusunda yönetime danışmanlık yapmak) |

İç denetim, yukarıdaki tabloda sınıflandırılan danışmanlık ve katılımcı rollerini, ancak bir önceki bölümde üzerinde durduğumuz iç denetçinin bağımsızlığını koruyan koşulların sağlanması şartına bağlı olarak işletme yönetimi ve iç denetçi arasında sağlanan konsensüs ile üstlenebilir. İç denetim fonksiyonunun söz konusu sorumlulukları üstlendiği iç denetim yönetmeliğinde ve organizasyon el kitabında açıkça ifade edilmelidir. Buna karşın iç denetimin üç hatlı savunma modeli bakış açısıyla, YRU kapsamında üstlenmemesi gereken temel sorumluluklar Tablo 3.13'te özetlenmiştir (Huibers, 2014, s. 20).

**Tablo 3.13.** *İç Denetimin Üstlenmemesi Gereken YRU Sorumlulukları (Huibers, 2014)*

| | |
|---|---|
| **YRU Kapsamında Üstlenilmemesi Gereken Sorumluluklar** | Risk iştahının belirlenmesi<br>YRU süreçlerini uygulamaya koymak<br>Kalite güvencesinde tanımlanan risklerin yönetiminde karar verici olmak<br>Önerilen çözümler ile ilgili yönetimsel kararlar almak<br>Yönetim adına karar verilen çözümleri uygulamaya koymak<br>YRU'ya ilişkin proje çıktılarından sorumlu olmak<br>YRU'ya ilişkin projelerin işletmede uygulanmasından sorumlu olmak |

IIA, anket ve görüşme tekniklerini kullanarak hazırladığı çalışma sonucunda, YRU uygulayıcılarına, ilgili taraflara ve diğer paydaşlara bir referans noktası sunabilmek amacıyla araştırma katılımcılarının üzerinde fikir birliği ettiği iyi YRU pratiklerini elde etmiştir. İyi pratiklere dayanarak, iç denetçiler ve diğer uygulayıcılar kendi uygulamalarında fayda elde etmek için YRU konusunda görüşlerini geliştirebileceklerdir. YRU yaklaşımının geliştirilmesi, sorumlulukların belirlenmesi ve kapsamı için yol gösteren iyi pratikler şunlardır (Man vd., 2010, s. 5):

- İç denetim biriminin, diğer risk ve kontrol birimlerinin görevleri ve pozisyonları üç hatlı savunma modeline göre belirlenir.
- İç denetim birimi YRU'yu denetim komitesine ve yönetim kurulu başkanına raporlar.
- Denetim komitesinin YRU'ya ilişkin görevleri açıkça ifade edilir.
- Uluslararası organizasyonlarda bile risk ve kontrol birimleri yerel yasalara ve düzenlemelere uygun şekilde kurulur ve YRU alanında yerel iyi pratikler göz önünde bulundurulur.
- İç denetim biriminin performansı, bağımsız denetçiler ve bağımsız kalite araştırmacılarının hazırladığı veriler kullanılarak, denetim komitesi tarafından değerlendirilir.
- İç denetim birimi, işletme birimlerinde YRU süreçlerinin uygulanışından daha çok, bu süreçlerin sonuçları ve performansı üzerine odaklanır.
- İç denetim birimi, işletme içinde otomatik kontrol modellerinin (sürekli denetim) uygulanmasına aktif şekilde destek olur.
- İç denetim birimi başkanı, eğer mümkünse, risk komiteleriyle toplantılar yapar.
- Risk değerlendirmede, iç denetim biriminin sorumluluğu sınırlıdır, ilke olarak, bu sorumluluk ilk hattın ve ikinci hattın (üç hatlı savunma modeli) üzerindedir.
- Yönetim kurulu işletmenin risk profilini ve risk yaklaşımını geliştirir.

- Tüm risk ve kontrol birimleri risk tespiti ve kontrol amacıyla, işletme çapında bütünleşik bir risk yönetimi sisteminden faydalanır.
- İç denetim birimi, risk yönetimi sisteminin karmaşıklığını azaltma konusunda açıkça katkıda bulunur.

IIA'nın çalışması sonucunda, YRU yaklaşımının geliştirilmesi, sorumluluklar ve kapsamının yanında, geliştirilen yaklaşımın işletme içinde uygulanması konusunda da iyi pratikler elde edilmiştir (Man vd., 2010, s. 6):

- İç denetim birimi analizlerinde ve tavsiyelerinde maliyet kontrolünü hesaba katar.
- İç denetim birimi, kendi birimi ve diğer risk ve kontrol birimleri için sürekli ve aktif şekilde çalışır.
- İç denetim birimi istenilen etkilere ulaşılması için proaktif bir şekilde çalışır.
- Kontroller test edilirken, yönetimle koordinasyon içinde, bütün taraflar incelenerek kapsam belirlenir.
- İç denetim birimi yönetişim ve kontrol çevresi ilişkisinde, işinin bir parçası olarak düzenli bir şekilde kültür ve yönetim tarzı gibi konuları değerlendirir.
- İç denetim birimi, işletmedeki farklı kültürel geçmişlerin farkındadır ve bunları çalışma yöntemlerinde ve raporlamada göz önünde bulundurur.
- İç denetim birimi, risk ve kontrol birimlerini, en iyi kontrollerin oluşturulması amacıyla sürekli olarak dikkatlice incelemelidir.
- İç denetim birimi, işletmede uygunluğu şeklen yasaları ve düzenlemeleri yerine getirmekten daha fazlası olarak değerlendirir. Sadece şekil değil, içerik te dikkate alınır ve bu durum yönetimin ve çalışanların sözlerinde ve davranışlarında da vurgulanmalıdır.
- Eğer işletme bütünleşik bir risk yönetimi sistemine sahipse veya YRU yaklaşımını benimsemişse, iç denetim birimi, sistemin yeterli objektiflik ve bağımsızlıkla değerlendirilebilmesi için önlemler alır.

### 3.12.5. YRU süreçlerinin iç denetiminde koordinasyon

İç denetçiler yönetişim, risk ve uygunluk (YRU) süreçlerinin geliştirilmesi ve işletme içinde YRU yaklaşımının benimsenmesi konusunda diğer çalışanlarla işbirliği halinde olmalıdır. Güçlü işbirliği ve koordinasyon, YRU başarısında etkilidir.

#### *3.12.5.1 İç denetimin diğer güvence birimleriyle koordinasyonu*

İç denetçiler YRU'ya güvence sağlayan tek grup değillerdir. Kendi alanlarında objektif bir denetim yürüten savunmanın ikinci hattındaki birimlerde (risk, kontrol, uygunluk, BT gibi) bulunan işletme içindeki çalışanlar da güvence sağlama görevini üstlenirler. Uluslararası İç Denetim Performans Standardı 2050, iç denetçilerin kendileri dışında denetim görevini üstlenen çalışanlarla işbirliğini düzenler. Buna göre, İç Denetim Yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgarîye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, ilgili güvence ve danışmanlık hizmetlerini yerine getiren diğer iç ve dış sağlayıcılarla, mevcut bilgileri paylaşmalı ve faaliyetleri bunlarla eşgüdüm içinde sürdürmelidir (IIA, 2010a, s. 14). YRU denetimi, iç denetimin işletme içinde diğer güvence vermeden sorumlu çalışanlarla koordinasyon sağlaması gereken alanlardan birisidir (Mefford, 2016, s. 42).

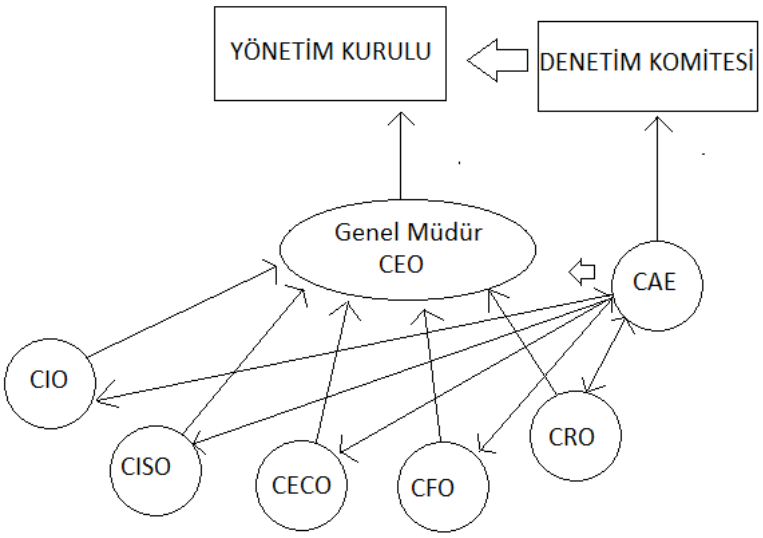
İç denetim dışında kalan diğer güvence çalışanlarının sık sık dile getirdiği bir konu, iç denetimin yaptığı çalışmaların kendileri tarafından zaten yapıldığıdır. İç denetçiler, denetimde etkinliği ve verimliliği sağlamak için ikinci savunma hattındaki birimlerin kontrol alanlarının denetlenmesi yerine, zaten bu birimlerce yapılan denetim işini göz ardı ederek, denetlenen alanlarda detaylı kontroller geliştirme aşamasına geçebilirler. YRU denetimini geliştirmenin en doğru yöntemi, denetimden sorumlu diğer birimlerle daha güçlü koordinasyon sağlamaktır. İç denetçilerin YRU denetiminde, diğer iç ve dış güvence sağlayıcılarla koordinasyonu ve işbirliğini sağlamasında en açık yol göstericiler, YRU çerçeveleridir. Örneğin, OCEG YRU Yetenek Modeli bu işbirliğinin kapsamını açıkça belirler (Mefford, 2016, s. 42).

#### *3.12.5.2 İç denetim birim yöneticisinin (CAE) sorumlulukları ve diğer güvence fonksiyonlarıyla işbirliği*

CAE, YRU süreçlerinin etkinliğine güvence sağlayan ve işletmenin karşılaştığı riskleri kontrol altına alan risk tabanlı bir denetim yaklaşımının benimsenmesinden sorumludur. CAE; çalışanlar, süreç, teknoloji ve kültürden oluşan dört temel operasyonel

boyutun tamamında değişimi getiren YRU yaklaşımının stratejik olarak tasarımında önemli bir taraftır. Her şeyin merkezinde yer alan CAE, hem stratejik hem de operasyonel seviyede YRU yaklaşımının etkilerini anlamalı ve işletmenin YRU stratejisinden en yüksek değeri elde etmesi amacıyla rehberlik etmeye hazır olmalıdır.

İyi tanımlanmış ve BT ile desteklenmiş iç denetim fonksiyonu, YRU için olmazsa olmazdır. Olmadığı zaman, yönetişim ve stratejik planlama zayıflar ve uygunluk yönetimi kaynakların uygunsuz tahsis edilmesi nedeniyle tehdit altındadır. Basit bir ifadeyle, etkili denetimin planlanması ve yönetimi, gerçek anlamda YRU stratejisinin merkezinde yer alır. Günümüzde, denetim ekibi tüm organizasyonda yönetişim, risk yönetimi, uygunluk ve kaynakların korunmasına olanak sağlar. Güçlü bir denetim yönetimi sürecini geliştirmek ve sürdürmek için, iç denetim birimi yöneticisi (CAE) yürütmeden sorumlu kilit yöneticilerle (genel müdür (CEO), riskten sorumlu yönetici (CRO) vs.) bilgi paylaşımında bulunmalı ve onları desteklemelidir (Şekil 3.26) (OCEG, 2016, s.7).




**Şekil 3.26.** *CAE'nin diğer C Seviye Yöneticiler ile ve Yönetim Kuruluyla İşbirliği*

CAE diğer fonksiyonlardan sorumlu yöneticiler ve üst yönetimle işbirliği yaparak temelde aşağıda sıralanan soruların cevaplarını arar:

1. BT ile desteklenen denetim yoluyla üretkenlik, şeffaflık ve karar alma nasıl geliştirilebilir?

2. İç ve dış paydaşlarla ilişkilerde yönetişim, risk ve uygunluğu destekleyen bütünleşik bir program ve ortak bir vizyon nasıl geliştirilebilir ve yüksek katma değer yaratacak şekilde nasıl uygulanabilir?
3. Denetim sürecinin verimliliği nasıl arttırılabilir ve stratejik amaçların yanı sıra diğer güvence fonksiyonlarıyla uyumlu bir plan nasıl elde edilebilir?
4. İşletmenin tümünde denetim faaliyetlerinde işbirliği nasıl güçlendirilebilir ve sınırlı denetim kaynaklarından verimli olarak faydalanılması nasıl sağlanabilir?
5. İşletme performansını destekleyebilen fırsatlar açığa çıkarılırken, kontrollerin etkinliğini arttıran ve daha güçlü bir risk farkındalığı yaratan bir denetim faaliyeti nasıl geliştirilebilir?

CAE ve denetim ekibi YRU faaliyetlerinin kalbinde yer alan politikalar, yordamlar ve sistemleri kapsayacak şekilde geleneksel finansal kontrollerden çok daha fazlasını anlamalı ve değerlendirmelidir. CAE, ortaya çıkan riskler hakkında daha fazla danışmanlık rolü üstlenmeli ve tasarlanan kontrollerin etkinliğini değerlendirmelidir. CAE ve denetim ekibi, risk yönetimi ve denetim sorumluluklarını genişleterek, değer yaratma ve yaratılan değeri koruma konusunda üst yönetime daha fazla yardım edebilirler. İşletmenin strateji ekibinin merkezinde yer alan anahtar bir çalışan olarak CAE, geniş kapsamlı paydaş taleplerini ve endişelerini göz önünde bulundurmalı ve aşağıda sıralanan sorunları gidermeye çalışmalıdır (OCEG, 2016, s.7-8).

- Anahtar paydaşların (yatırımcılar, düzenleyici kurumlar, sivil toplum kuruluşları, yerel topluluklar) şeffaflık talebi,
- Yönetim kurulu ve üst yöneticilerin gelecekte sonuçları etkileyebilecek ve stratejik kararları yönlendirecek önemli konular ve riskler hakkında açık ve güvenilir bilgi ihtiyacı,
- Uygunluk ve hukuk birimi yöneticilerinin önemli riskleri azaltma amacına yönelik proaktif kontrollerin, bulma kontrollerinin ve tepkisel kontrollerin kurulması amacıyla sınırlı kaynakların tahsis edilmesi ihtiyacı,
- İşletmede birçok denetim grubu ve faaliyeti arasında daha iyi işbirliği ve koordinasyon,
- İşletmenin tamamında riskleri azaltmak ve eksiklikleri gidermek amacıyla temel ihtiyaçlar.

CAE, sürdürülebilir bir YRU stratejisini uygulayarak ve temel riskleri anlayarak birimler arası BT destekli bir denetim programının geliştirilmesine katkı sağlayan bir

görüşmeler serisi yoluyla işletmeyi yönlendirmelidir. CAE, aşağıda sıralanan görevleri mümkün olduğunca yerine getirmeye çalışmalıdır (OCEG, 2016, s. 9):

- Yönetim kurulu ve üst yönetime, şirket genelinde riske dayalı bir denetim programının stratejik hedefleri tanımlama ve bunlara ulaşmada kritik önem taşıdığını açıkça ifade etmelidir.
- İşleri idare etmek için risk bilgisiyle karar alırken genel müdüre (CEO) destek olmalıdır.
- İşletmeyi stratejik ve operasyonel amaçları için yönetirken sürekli olarak fırsatları değerlendirmelidir.
- Risk ve kontrol analizlerini geliştirirken, risk ve denetim yaklaşımındaki değişimleri yönlendirecek şartları raporlarken ve tavsiyeler getirirken kilit üst yöneticilerin desteğini kazanmalıdır.
- İşletme çapında risklerin ve kontrollerin açık ve uygun bir görünümüne sahip olmanın, stratejik amaçları belirlemede ve bunlara ulaşmada neden önemli olduğunu yönetim kuruluna ve üst yönetime açıkça ifade etmelidir.
- Uygunsuzluk ve olumsuz sonuçlarla karşılaşma riskini azaltmak için çalışanların belirlenen sınırlar içerisinde hareket etmesine olanak sağlayan işletme çapındaki risk kültürünü geliştirirken ve risk yaklaşımını belirlerken yönetim kurulu ve üst yönetime yardım etmelidir.
- Birimler seviyesine dağıtılan YRU stratejisinin uygulanmasında diğer kilit fonksiyonel yöneticiler ile işbirliği yapmalıdır.
- İşletme performansının bütün yönlerini değerlendirmek için kullanılabilen farklı perspektifleri toplayan kontrollerin etkinliğini ve risklerin bütüncül bir görünümünü sağlayan risk tabanlı denetim programlarının ne kadar güçlü olduğunu çalışanlara ve yöneticilere göstermelidir.
- İşletmenin tedarikçilerin, üçüncü tarafların ve müşterilerin yer aldığı giderek karmaşıklaşan ekosistemde bulunan risklerin proaktif bir şekilde kontrol altına alabilmesi için, sağlam bir analitik çerçevenin nasıl faydalı olabileceğini göstermelidir.
- BT destekli bir denetim programının gerçek zamanlı risk anlayışı sayesinde üretkenliği desteklemeye, şeffaflığı ve karar almayı geliştirmeye nasıl katkı sağlayacağını tartışmalıdır.

- İşletme çapında kapsamlı bir BT destekli denetim programı tanımlamalı, hedeflenen denetim programı doğrultusunda ekibi yönlendirmeli ve verimli bir denetim saha çalışması ve etkili raporlama yoluyla YRU süreçlerine etkin güvence sağlamaya çalışmalıdır.

#### *3.12.5.2.1. Yönetim kurulu ve genel müdür (CEO) ile işbirliği*

Yönetim kurulu, belirli bir projeden sorumlu komite veya CEO gibi herhangi bir yönetişim otoritesinin temel görevi, bir faaliyeti veya işletmeyi yönetenler tarafından sağlanan yönlendirme ve kontrolden bağımsız olarak gözetim sağlamaktır. Gözetim, yöneticilerin ve denetçilerin görevlerini yerine getirirken kullanacakları yönlendirme ve karar verme ölçütlerini sağlamayı içerir. Bu misyonun, vizyonun ve değerlerin yanı sıra risk yaklaşımı, risk toleransı, etik rehberler ve yüksek düzeydeki amaçların belirlenmesini kapsar. Bazı durumlarda, yönetim otoritesi stratejik planlamayı geliştirir ve yönlendirir; stratejik planları hazırlar veya onaylar. Amaçlar, karar verme ölçütleri ve stratejik planlardaki değişiklikler karşılıklı olarak ihtiyaçlar, tehditler ve fırsatlar hakkında uygun iletişimi sağlayabilmeleri için üretimden sorumlu yöneticilere, risk ve uyum yöneticilerine ve denetçilere zamanında bildirilmelidir. Planlar, yeterli kaynak tahsisi yapılması ve tasarlanan stratejik planlarla ilişkili eylemler ve kontroller geliştirilmesi için faaliyet birimleri, insan kaynakları, finans ve diğer birimlerdeki kişilere de sağlanmalıdır (OCEG, 2015a, s. 7).

CAE; yönetim kuruluyla, risk ve uygunluk yönetimi yaklaşımının işletmeyi ilkeli performansa yönlendiren YRU stratejisine dayanmasını sağlayan ve işletmenin risk yaklaşımına rehberlik eden etkili bir denetim komitesi kurmak amacıyla işbirliği yapmalıdır. İç denetim birimi, yönetim kuruluna standartlaştırılmış kilit ölçümleri kullanarak denetimde güvenilirliğin sağlanmasına dayanan teknoloji temelli bir denetim programının, işletme amaçlarına daha kolay ulaşılmasına nasıl imkan sağladığını göstermelidir. Denetimin daha iyi yönetilmesinin, kontrol zayıflıklarının ve diğer önemli sorunların belirlenmesini de kapsayacak şekilde risklerin ve kontrollerin daha iyi yönetilmesini sağlayacağını, böylece hem verimliliğin geliştirilmesiyle hem de kontroller uygulandıktan sonra bile varlığını sürdüren artık (bakiye riski) risklerin daha kapsamlı anlaşılmasıyla sonuçlanacağı açıklanmalıdır (Delmar vd., 2016, s. 15).

CAE, işletmeyi giderek dijitalleşen ve çok hızlı evrilen küresel ekosistemdeki stratejik önceliklerine uygun olarak yönetmesi için, CEO'nun yanında daimi bir danışman

olmalıdır. İç denetimin düzenlemelerin gerekliliklerini ve işletme stratejisini anlaması, CEO'nun işletmeyi ilkeli performansa yönlendirirken riski dikkate alarak eylemlerde bulunmasına yardımcı olur. İç denetim programı, risk hakkında tavsiyeler sağlar ve önemli riskleri etkili biçimde ele alıp fırsatlardan faydalanılabilecek alanları belirleyerek CEO'ya destek olur. İç denetim, işletme yönetimi ve işletme planlama döngüsünde destekleyici süreçler ve sistemler ile sürdürülebilir, bütünleşik bir YRU yaklaşımının kurumsallaştırılmasında CEO'dan destek almak zorundadır. Bu destek, ilkeli performansa giden yolda önemli bir adımdır (OCEG, 2016, s.9).

#### *3.12.5.2.2. Finanstan sorumlu yönetici (CFO) ile işbirliği*

Modern CFO'ların işi, varlıkların korunması ve finansal kayıtların yönetilmesi olan geleneksel görevinin çok ötesine geçmiştir. Bugün, CFO strateji ekibinin önemli bir üyesidir ve işletmenin finansal kaynaklarının uygun şekilde tahsis edilmesini sağlayarak işletmenin doğru yönlendirilmesine katkıda bulunur. CFO, işletmenin finansal anlayışıyla ilişkili karar verme ölçütlerini belirleyerek ve açıklayarak yönetimin daha iyi faaliyet göstermesine yardım etmelidir. Stratejinin ötesinde, iş geliştirme girişimlerini seçici bir şekilde kurup destekleyerek, işletmenin gelişimini yönlendirir. CFO'nun desteklenmesi, YRU başarısı için çok önemlidir (OCEG, 2015a, s. 7).

Risk yönetimi ve hissedar değeri arasındaki bağlantı, YRU yaklaşımı ve stratejisinin bir parçası olan denetim yaklaşımının geliştirilmesini sağlamak amacıyla iç denetim birimi yöneticisi (CAE) ile CFO'nun yakın çalışması ve işbirliği yapması gereken bir konudur. CAE, yapılandırılmış bir güvence yaklaşımının finansal performansı nasıl artırdığını CFO'ya göstermelidir. Riskin izlenmesi ve iç denetim sorumluluklarının yerine getirilmesinin işletmede sadece değer yaratmayı değil aynı zamanda da yaratılan değeri nasıl koruduğu CFO'ya açıklanmalıdır. Birleşme ve devralma, birleşme sonrası faaliyetler, stratejik kaynak sağlama ve operasyonel faaliyetleri izleyerek denetimin değer yaratması noktasında iç denetim, CFO ile işbirliği yapmalıdır.

Planlanan anahtar girişimlerin bilinmesinin yanı sıra işletmenin amaçlarının ve stratejilerinin anlaşılmasının, iç denetimin işletmenin risk profilini temel alan etkili bir risk tabanlı denetim planını geliştirmesine nasıl imkân sağlayacağına dair CFO ile uzlaşılmalıdır. Ayrıca, iç denetimin riskin anlaşılması ve riski dikkate alarak işletmenin nasıl yönetileceği konusunda üst yönetime danışmanlıkta bulunma, uygun bir kontrol

ortamı oluşturulması için planlama yapılması ve piyasa düzenleyici normların öğrenilmesinde nasıl kilit rol üstlenebileceği CFO'ya açıklanmalıdır. Bu ihtiyaç iç denetim ile CFO arasında düzenli bir iletişimi gerektirir, böylece iç denetim izleme ve kontrollerin arttırılması gereken yüksek riske maruz kalan alanları bilebilir, risk faktörlerini daha iyi belirleyebilir ve kontrol edebilir, denetim ve risk yönetimi süreçlerini örgütsel faaliyetler ve amaçlardaki değişikliklere cevap verebilecek şekilde düzenleyebilir. YRU stratejisinin uygulanmasında CAE ve CFO'nun karşılıklı faydaya dayanan ilişkisi açıkça belirlenmelidir (Delmar vd., 2016, s. 16).

Genel olarak işletme riskleri; aynı zamanda birbirlerini etkileyen stratejik, finansal, operasyonel, ticari ve teknik faktörlerden kaynaklanır. İç denetim ve CFO, işletme çapında risklerin bütüncül bir görünümünü ve denetim görüşleri ve tavsiyeleriyle birlikte kontrollerin etkinliğini sağlayan raporlama yapısını ve anahtar riskleri gidermeye çalışan genel denetim stratejisini planlarken nasıl birlikte çalışacaklarını tartışmalıdırlar. Ayrıca, işletmenin değer yaratmasına ve yarattığı değeri korumasına destek sağlayacak olan denetim yaklaşımını oluştururken, ihtiyaç duyacağı kaynaklar iç denetimin olduğu gibi CFO'nun da sorumluluğundadır (OCEG, 2016, s.10).

#### *3.12.5.2.3. Riskten sorumlu yönetici (CRO) ile işbirliği*

CRO ve risk yöneticileri, KRY veya işletme fonksiyonları özelinde risk ve kontrol çabalarından hangisiyle uğraşırlarsa uğraşsınlar, işletmenin ilkeli performansa yönlendirilmesinde olmazsa olmaz bir unsur olarak rol oynarlar. Hem CRO'nun altındaki hem de diğer işletme birimlerindeki risk ekipleri, işletmeye sunulan fırsatları ve tehditleri göz önünde bulundurmalı ve stratejik planlar geliştirildiğinde ve uygulandığında bu bilgilerin mevcut bulunmasını sağlamalıdırlar. İşletme yönetimi, riski dikkate alan karar alma süreçlerini kurumsal çapta bütünleştirmelidir. Belirlenen amaçlar ve stratejiler ışığında tehditleri kontrol etme ve fırsatları keşfetme, denklemin yalnızca bir parçasıdır. İç ve dış değişikliklerden kaynaklanan herhangi bir dalgalanmanın amaçların başarılmasını nasıl etkileyebileceğini değerlendirmek eşit derecede önemlidir. Bu süreç, stratejik planlamacılar ve yönetişim otoriteleriyle iletişim halinde yapılmalıdır. Ayrıca risk değerlendirme bir yaptım ve bitti faaliyeti değildir; amaçlar, stratejiler, riskler, ödüller ve kontroller arasındaki uyumun devam etmesini sağlamak için, değişimin ve farklılıkların sürekli olarak izlenmesi gerekir (OCEG, 2015a, s. 8).

CAE ve CRO, işletme faaliyetlerini derinden etkileyen işletmenin risk profili hakkında denetim ve risk ekiplerinin görüşlerinin nasıl uyumlaştırılacağını ve denetim ile risk yönetimi ekipleri arasındaki sinerjinin yönetime önemli risk alanları hakkında nasıl açık fikirler sağlayabileceğini ve ortaya çıkan fırsatlardan nasıl faydalanılabileceğini tartışmalıdır. Bu iki fonksiyon arasındaki işbirliği, gerekli bilginin elde edilmesine ve daha sonraki raporların uyumlaştırılmasına hız kazandırır. Kontroller ve risklere ilişkin kapsamlı raporlar, düzenlemelerle dolu işletme çevresinde yaşanan değişikliklerin üstesinden gelmek için en uygun ve etkili önlemlerin seçilmesine imkân sağlayan zamanında karar almayı ve riskin ihtiyaç duyulan iletişim kanallarıyla yönetilmesini sağlayacaktır (OCEG, 2016, s.11).

#### *3.12.5.2.4. Etik ve uygunluktan sorumlu yönetici (CECO) ile işbirliği*

CECO ile diğer uygunluktan ve etikten sorumlu yöneticiler, yalnızca işletmenin uymakla yükümlü olduğu yasal gerekliliklerle değil aynı zamanda da işletmenin kendi içinde geliştirdiği değerler, politikalar, yordamlar ve davranış kurallarına uyulmasıyla da ilgilenmelidirler. Bunlar gönüllü ve zorunlu sınırlar olarak tanımlanabilir ve bu ekibin işi işletmenin (birimin veya projenin) amaçlarına ulaşmak için çabalarken bu sınırların içinde kalındığından emin olunmasıdır. Sınırların aşılmaması, yönetim eylemleri ve kontrollerinin bir karışımının uygulanmasıyla sağlanır ve risk yönetiminde olduğu gibi, bu eylem ve kontroller sadece stratejiyi desteklemekle kalmaz aynı zamanda onu etkileyebilir. Uyum yönetimi sorumluluğuna sahip olanların, önce stratejik değişim planlarını öğrenmeleri esastır. Normal şartlarda, kararları etkileyebilecek bilgilerin iletişimini sağlamak için planlama tartışmalarına dahil olmalıdırlar. Benzer şekilde, uygunluk ve etikten sorumlu çalışanlar ve risk çalışanları, sınırların içinde optimum seviyede kalmak amacıyla ihtiyaç duyulan kaynaklar, ortadan kalkan sınırlardan nasıl etkilenileceği ve uygunluk ihtiyaçlarının risk analizlerini nasıl etkileyeceği konuları hakkında iletişim halinde olmalıdırlar. Etik karar almanın geliştirilmesi konusunda insan kaynakları yöneticileriyle iletişim kurulması ve birlikte çalışılması da önemlidir (OCEG, 2015a, s. 8).

İç denetim ve uygunluk birimi işletme içinde farklı rollere ve gerekliliklere sahip olsalar da, YRU yaşam döngüsü içerisinde birbirleriyle bağlantılıdırlar. İç denetim ve uygunluk arasındaki güçlü bir bağlantı noktası, yönetim kuruluyla ilişkileridir. Her ikisi de yönetim kurulunu yönlendirir ve basit bir ifadeyle ikisi de benzer bir danışmanlık

hizmeti sunar. Hem iç denetim hem de uygunluk fonksiyonları, işletmeye özel riskleri değerlendirmek ve raporlamak için hesap verebilirliğe ve yönetim kuruluyla raporlama ilişkileri için gereken bağımsızlığa sahiptir. Birbirine bağlı raporlama ilişkilerinde, iç denetim ve uygunluğun ortak bir risk ve kontrol dilinden faydalanmaları ve üst yönetime daha uyumlu ve koordineli bilgi akışı sağlamak için raporlarında şeffaflığı geliştirmeleri çok önemlidir (Peak, 2012, s. 5).

İç denetim CECO'ya, risk tabanlı denetim yaklaşımının uygunluk amaçlarına ulaşılmasına yardım edecek ortak bir çerçevede düzenlemeler, politikalar, riskler ve kontrolleri planlamada kullanılan temel bilgilerden nasıl yararlanacağını göstermelidir. İç denetim, CECO ile uygunluk ihtiyaçlarını etkileme ihtimali olan işletme süreçlerindeki ve düzenlemelerdeki değişimlerin etkisini değerlendirmek amacıyla işbirliği yapmalıdır. Denetimin yeni veya değişen düzenleyici normları karşılamak için uygun bir kontrol ortamının planlanmasına ve maruz kalınan risklerin anlaşılması ve yönetilmesine nasıl katkı sağladığı CECO'ya açıklanmalıdır. CAE ve CECO, birçok düzenlemenin farklı işletme birimlerini farklı şekilde nasıl etkileyeceğini tartışmalı ve birçok ihtiyacı birden karşılayabilen kontrollerin yerlerinin nasıl belirleneceği hakkında konuşmalıdır. Ayrıca soruşturmaları, mahkeme çağrılarını, araştırmaları, rutin denetimleri ve dış incelemeleri ele almak için yerinde politikalar ile bütün sistemin denetime hazır hale getirildiği hakkında uzlaşmaya varılmalıdır. Uygunluk ve etik risklerin nasıl belirlendiği ve kontrol altına alındığı konusunda izleme faaliyetlerinin yürütülmesi ile CEO ve yönetim kuruluna düzenli olarak raporlama yapılması amacıyla iç denetim, uygunlukla ortak bir çalışma yürütmelidir (OCEG, 2016, s.11).

#### *3.12.5.2.5. Bilişimden sorumlu yönetici (CIO) ve bilişim güvenliğinden sorumlu yönetici (CISO) ile işbirliği*

CIO, işletmenin doğru bilgileri doğru kişilere veya sistemlere doğru zamanda ve doğru biçimde sunmasına izin veren yollarla bilgi toplamak ve bilginin sürekliliğini sağlamak için sistemler oluşturmalıdır. Bu YRU yaklaşımı için önemli bir faaliyettir. Bir işletmenin bilgi güvenliğini korumak ve gerekli teknoloji kaynaklarının ve bilginin kullanılabilirliğini sağlamak kritik önem taşır. CIO ve bilgi teknolojisi yöneticileri, kullanıcı ve paydaş ihtiyaçlarına dayalı doğru çözümlerin kombinasyonunu belirleyecek olan YRU teknolojisinin tasarlanmasına yardımcı olmalıdırlar. Daha sonra, şu anda hangi teknolojilerin kullanıldığını, nelerin korunması, değiştirilmesi veya bütünleştirilmesi

gerektiğini belirlemek için anahtar yöneticiler ile birlikte çalışmalıdırlar. Böylece, YRU yaklaşımı için tam olarak tasarlanmış bir teknoloji sağlanır (OCEG, 2015a, s. 9).

YRU stratejisinin, programının ve sisteminin başarısı için, bütünleşik risk değerlendirme ve denetim ile YRU teknolojisinin uygulanmasına yönelik özenli ve bilinçli bir yaklaşım önemli ve gereklidir. CAE ve CIO'nun görüşmesinde zamandan ve kaynaklardan tasarruf sağlamak amacıyla yapılması gerekenlerin anlaşılması, süreçlerin ve sistemlerin BT ortamında nasıl yürütülmesi gerektiği ve bilgi yapısının nasıl iyi tasarlanabileceği tartışılmalıdır. Otomatik kontrol testlerinin sonuçlarının ve ölçümlerinin anlaşılmasını ve yorumlanmasını destekleyen ve işletmenin riskleri tahmin etmesine ve karşılık vermesine yardım eden iyi tasarlanan ve yönetilen bilgi yapısı özellikle önemlidir. CAE ve CIO aşağıda sıralanan konularda işbirliği yapılmalıdır (OCEG, 2016, s.12).

- İşletme çapında teknoloji vizyonu, altyapı, risk ve kontrol gereklilikleri BT ile desteklenmek amacıyla belirlenmelidir.
- Gerçek zamanlı risk yönetimini sağlamak için dijital işletme, büyük veri ve bulut teknolojilerin etkisi anlaşılmalıdır.
- İşletmenin YRU ihtiyaçları belirlenmelidir ve ayrıntılı ihtiyaçlara en iyi şekilde cevap vermesi beklenen teknoloji ve bilgi yapısı değerlendirilmelidir.
- Kontrol tasarımı ve test programlarıyla desteklenen YRU süreçleri için işletme gerekliliklerinin teknoloji ortamında yürütülmesine olanak tanıyan sistem ve uygulamalara uyum sağlamak, işbirliğini geliştirmek ve YRU yazılımını kurmak için bir plan yapılmalıdır.

CISO ise işletme içinde önemli, düzenlenmiş ve hassas bilginin gizliliğini, doğruluğunu ve kullanılabilirliğini korumakla yükümlüdür. Özellikle siber tehditlerle ilişkili olarak bilgi güvenliğinde risk tanımlama, raporlama ve veri analizi yaklaşımları hızla dönüşüm göstermektedir. CAE bu yeni yaklaşımları anlamalı ve kontrol çerçevelerine uyarlamalıdır. CAE ve CISO; olay ve kriz yönetimi ekipleri, CIO ve diğer önemli işletme birimleriyle yakın işbirliği kurmalıdır. CAE ve denetim komitesi, CIO ve CISO'nun önemli siber güvenlik sorunlarını düzenli olarak tartışmalarını ve ortaya çıkan tehditler, siber güvenlik düzenlemeleri ve zayıflıklar konusunda bilgi paylaşımı yapmalarını sağlamak konusunda sorumluluk üstlenirler. CAE ve denetim ekibinden veri güvenliği tehditlerinden haberdar olmaları ve anlamaları beklenmektedir. Ayrıca zayıflıkların belirlenmesi ve risklerin en uygun seviyeye getirilmesi için sürekli olarak

çaba gösterilmesi gereklidir. CAE ve CISO aşağıda sıralanan konularda işbirliği yapmalıdır (OCEG, 2016, s.13).

- İşletme amaçları; kurumsal, operasyonel, bilgi teknolojileri ve güvenlik riskleri ile kontrollerine göre düzenlenmelidir.
- Bilgi güvenliği vizyonu, bilgi güvenliğini destekleyen denetim ve risk yönetimi gereklilikleri, fiziksel güvenlik ve siber tehditler belirlenmelidir.
- Güvenlik gereklilikleri belirlenmelidir, tanımlanan teknoloji ve bilgi yapısı ihtiyaçlarına en iyi şekilde cevap vermek amacıyla geliştirilen çözümler değerlendirilmelidir.
- Bilginin paylaşılabilmesi ve diğer kullanıcılar ile uyum sağlayabilen mevcut çözümlerin belirlenmesi amacıyla kullanılan güvenlik ve izleme sistemleri tanımlanmalıdır.

# 4. İÇ DENETİM SORUMLULUKLARININ YRU YAKLAŞIMINA ETKİSİ ÜZERİNE YAPISAL EŞİTLİK MODELİ ARAŞTIRMASI

Çalışmanın bu bölümünde, araştırma modelini oluşturan kavramsal çerçeve ve test edilen hipotezlere yer verilmiştir. Araştırmanın ana kütlesi ve örnekleminin demografik özellikleri tanımlanmış ve araştırmanın yöntemi açıklanmıştır. Çalışmanın, iç denetçilerin yönetişim, risk yönetimi, uygunluk ve teknolojiye ilişkin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini ölçmek amacıyla kurgulanan araştırma modeli betimlenmiştir.

## 4.1. Çalışmanın Literatürü ve Kavramsal Çerçevesi

Çalışmamızda YRU'nun temel bileşenleri olan yönetişim, risk yönetimi ve uygunluk ile YRU bileşenlerinin bir araya getirilmesi ve uygulanabilmesi için olmazsa olmaz olan teknolojiye ilişkin iç denetim sorumluluklarını belirlemek ve uygulamada sorumlulukların hangi düzeyde üstlenildiğini tespit etmek amaçlanmıştır. İç denetçilerin sorumluluklarının, YRU yaklaşımından beklenen faydalar üzerindeki etkisini ortaya çıkarmak amacıyla araştırma modeli geliştirilmiştir. Elde edilen görüşler, uygulamadaki durumla ve katılımcı grupları arasında karşılaştırmalı olarak incelenmiştir. İlgili literatür incelendiğinde yönetişim, risk yönetimi, uygunluk ve teknolojinin birbirinden bağımsız olarak iç denetim ile ilişkisini ve iç denetçilerin sorumluklarını ele alan birçok teorik ve deneysel çalışmanın olduğu belirlenmiştir.

### 4.1.1. İç Denetimin Yönetişim Sorumlulukları

Son yıllarda yeni yönetişim yaklaşımları, yönetim kurulunun işletmelerin iç kontrol çerçevesinin etkinliğini sağlamakla yükümlü olduğunu kabul etmiştir. Bu teoriler iç kontrollerin yeterli seviyede gözetimi ve yönetim kurulunun sorumluluklarını yerine getirme konusunda desteklenmesinde yönetişim çerçevesinin ayrılmaz bir parçası olan iç denetimin önemli görevler üstlenmesi gerektiğini vurgulamaktadır. Özellikle ulusal ve uluslararası ilke, düzenleme ve standartlar, iç denetimin yönetişim konusundaki rolüne önem kazandırmıştır. Literatürde iç denetim ile yönetişim arasındaki ilişkiyi araştıran teorik ve uygulamaya yönelik çalışmalar bulunmaktadır.

İç denetimin rolü yönetişimin teorik temelleri içine gömülüdür. Temel yönetişim teorisi olan Vekâlet Teorisine göre, hissedarlar ile yöneticilerin çıkarları ancak geliştirilen, uygulanan ve izlenen bir dizi kontrol vasıtasıyla uyumlaştırılabilir (Berle &

Means, 1932; Jensen & Meckling, 1976). Adams (1994) iç denetim fonksiyonunun, bu kontrollerin yönetim kurulu adına sürekli olarak izlenmesinde önemli bir role sahip olduğunu savunmuştur. Bu bağlamda iç denetim fonksiyonu, denetim komitesi aracılığıyla yönetişim odaklı kontrollerin etkinliği ve uygunluğu konusunda yönetim kuruluna güvence sağlar.

İç denetim mesleği, iç denetim fonksiyonunun önceliğini, yönetişim paradigması içindeki sorumluluklarına çevirmiştir. 1999'da iç denetimin gözden geçirilmiş tanımı ile meslek, iç denetimin yönetişimin geliştirilmesinde önemli rol oynadığını kabul etmiştir. Bu tanımla birlikte iç denetimin rolü, yönetim kuruluna ve üst yönetime, yönetişim süreçlerinin yeterliliği konusunda güvence sağlayacak şekilde genişlemiştir. Bu yeni rol iç denetimin işletmeye katma değer sağlayan üst yönetime danışmanlık görevlerinin önemini artırmıştır (Fraser & Henry, 2007; Page & Spira, 2004). İç denetimin bu bağlamdaki rolü meslek tarafından etkili yönetişimin temel taşı olarak kabul edilmiştir.

İç denetimin genişleyen rolüyle birlikte yönetişimin önemli bir bileşeni haline geldiği ve iç denetim biriminin yönetişimin ayrılmaz bir parçası olduğu görüşü araştırmacılar tarafından desteklenmiştir (Rittenberg & Anderson, 2002; Ruud, 2003). Daha sonra yapılan çalışmalar da bu tutumu doğrulamıştır (Carcello vd., 2005; Goodwin-Stewart & Kent, 2006; Paape vd., 2003). İç denetim mesleğinde yaşanan gelişmeler, iç denetimin yönetişim çerçevesinde belirgin bir rol üstlenmesine sebep olmuştur. Bu rol yönetişim konusunda yapılan çalışmalar, uygulamalar, yasal düzenlemeler ve rehberler tarafından desteklenmiştir. Birçok yönetişim komitesi işletmelerin iç denetim birimi kurmalarını teşvik etmektedir (Cadbury, 1992; COSO Report, 1992). Kamu ve özel sektör işletmelerinin yönetim kurulları ve üst yöneticileri, iş dünyasında yaşanan gelişmelerin sonucu olarak, yönetişim sorumluluklarını yerine getirmede giderek iç denetime bağımlılık göstermektedir (Christopher, 2015, s.956).

Birçok çalışma iç denetimi yönetişim mekanizmasının kalitesini arttıran bir değişken olarak incelemiştir. Beasley vd. (2000) iç denetim fonksiyonuna sahip olan işletmelerde hileli işlemlerin yaşanma olasılığının diğer işletmelere göre anlamlı seviyede düşük olduğunu raporlamıştır. Cohen vd. (2002) yaptığı çalışmada, katılımcıların yüzde 90'ının iç denetimin yönetişimi olumlu yönde etkileyeceğini düşündüklerini ancak mevcut iç denetim birimlerinin gücüyle ilgili endişelerinin var olduğunu keşfetmiştir. Goodwin & Seow (2002) iç denetim, denetim komitesi ve yönetişim kodları gibi değişkenlerin yönetişim üzerindeki etkisini araştırmıştır. Denetçiler ve üst yöneticiler

üzerinde yapılan anket çalışmasından elde edilen verilere göre iç denetim, işletmede özellikle hilenin önlenmesi ve finansal raporlamanın kalitesinin artırılması gibi katkılar sağlayarak yönetişimi olumlu etkiler.

Paape, Scheffe & Snoep (2003), Avrupa İç Denetçiler Enstitüsü Konfederasyonunun (ECIIA) şirketleri borsada işlem gören üyeleri üzerinde yaptıkları anket çalışmasıyla, iç denetim fonksiyonu ile yönetişim arasındaki ilişkiyi ortaya çıkarmaya çalışmıştır. Elde edilen veriler, Avrupa'da faaliyet gösteren büyük ölçekli işletmelerin iç denetçilerinin çalışma şekillerinde şaşırtıcı farklılıklar olduğu ve yönetişim mekanizmasını etkileyen farklı görevler üstlendikleri sonucunu ortaya çıkarır.

Abdioğlu (2007), doktora çalışmasında borsaya kote şirketlerde iç denetimin yönetişim anlayışı kapsamında rolünü ortaya çıkarmaya çalışmıştır. İç denetimin yönetişimin bir parçası olduğu ve iç denetim aracılığıyla yönetişim anlayışının işletmeye sağlamayı amaçladığı faydalara daha kolay ulaşılacağı belirlenmiştir. İç denetim yönetişim ihtiyaçlarına cevap verebilmek amacıyla niteliklerini geliştirmelidir.

Elbannan (2009), iç denetim kalitesinin yönetişim üzerindeki etkisini araştırmıştır. İki değişken arasında pozitif yönlü ilişki saptanmıştır. Ayrıca yönetişimin geliştirmeyi amaçladığı işletmenin kredi notunun, iç denetim kalitesinin bir fonksiyonu olduğunu belirlemiştir.

Usul, Titiz & Ateş (2011), iç denetimin yönetişimin geliştirilmesindeki etkisini belediyelerden oluşan bir örneklemde test etmiştir. İç denetimin yönetişimi etkileyen alanlarda yaptığı çalışmalar incelenmiştir. Bu bağlamda söz konusu örneklemde iç denetimin yönetişimi etkileyen görevlerini gerektiği gibi üstlenmediği ve yönetişim anlayışının geliştirilemediği sonucuna ulaşılmıştır.

Küpçü (2011), yönetişim ile iç denetim arasındaki ilişkiyi Türkiye'de faaliyet gösteren örnek bir işletmede yönetişimde iç denetimin rolünü belirleyerek ortaya koymaya çalışmıştır. Sonuç olarak iç denetimin yönetişimin sigortası olduğu ve mesleğin rolünün gelecekte daha da artacağı tahmin edilmiştir.

Cengiz (2013), BİST-100 endeksinde yer alan şirketlerden oluşan örnekleminde, yönetişim kapsamında iç denetimin yeri ve önemini anket aracılığıyla ortaya çıkarmaya çalışmıştır. İç denetimin yönetişim uygulamalarının merkezinde olduğu ve üst yönetime yönetişim süreçlerinin yeterliliği konusunda değerlendirmeleriyle güvence sağladığı sonucuna varılmıştır.

### 4.1.2. İç Denetimin Risk Yönetimi Sorumlulukları

Kurumsal Risk Yönetiminde iç denetim fonksiyonunun sorumlulukları konusunda IIA Araştırma Vakfı'nın yayımladığı iki çalışma ilk bakış açısını yansıtmaktadır. Tillinghast-Towers (2004), iç denetçiler ve diğer işletme yöneticilerinden oluşan örneklem üzerinde anket çalışması gerçekleştirmişlerdir. Çalışma sonuçlarına göre işletmelerin yüzde 32'sinde iç denetçiler KRY çalışma ekiplerine katılmıştır. Anketin odak noktasında işletmede KRY uygulamaları yer alır. İç denetim KRY sorumluluklarını sınırlı şekilde ele almıştır. Walker vd. (2002) yaptıkları çalışmada beş büyük organizasyonun (First Energy Corporation, General Motors, Unocal, WalMart ve Canada Post Corporation) KRY süreçlerinde iç denetimin rolüne dair tanımlayıcı bilgilere yer vermiştir. Çalışmada KRY uygulamasının temel unsurları tanımlanmış ve iç denetçilerin işletmelerde oynadığı KRY rolü vaka analiziyle incelenmiştir. İç denetim fonksiyonunun söz konusu beş işletmede KRY süreçlerine farklı biçimlerde de olsa katıldığı belirlenmiştir. İç denetim fonksiyonu özellikle risklerin belirlenmesi ve risk raporlarının hazırlanmasında önemli sorumluluk üstlenmiştir (Walker vd., 2002, s.16).

Beasley vd. (2005) küresel organizasyonlarda KRY'nin benimsenme durumu ve iç denetimin KRY sorumluluklarına ilişkin tanımlayıcı istatistikler sunmuştur. Çalışmada ankete katılan işletmelerin yüzde 48'inin kısmen ya da tamamen geliştirilmiş KRY çerçevelerine sahip olduğu tespit edilmiştir. Ayrıca iç denetim fonksiyonunun riskten sorumlu yönetici (CRO) ile yakın ilişkiler geliştirdiği, işletme içinde çeşitli taraflar arasında KRY çalışmalarının koordinasyonu, risklerin belirlenmesi, kontrol faaliyetlerinin geliştirilmesi ve KRY süreçlerinin izlenmesi konularında görevler üstlendiği belirlenmiştir.

Gramling & Myers (2006), IIA'nın 2004 yılında yayımladığı iç denetimin KRY süreçlerinde rolü raporunda tanımladığı sorumluluklar ile uygulamada söz konusu sorumlulukların ne seviyede üstlenildiğini karşılaştırmıştır. IIA'nın belirlediği iç denetimin KRY süreçlerindeki temel rolleriyle ilgili konularda katılımın orta düzeyde olduğu, belirli şartlar altında sahip olunabilecek rollerle ve sahip olunmaması gereken rollerle ilgili konularda katılımın sınırlı olduğu sonucuna varılmıştır. Genel olarak, birçok işletmede iç denetimin yürüttüğü KRY faaliyetlerinin, IIA raporlarıyla büyük oranda uyumlu olduğu belirlenmiştir.

Beasley vd. (2006) kurumsal risk yönetiminin iç denetim fonksiyonunun faaliyetleri üzerindeki etkisiyle ilişkili faktörleri incelemiştir. Farklı ülkelerdeki 122

işletmeden elde edilen verilere göre, KRY'nin iç denetim faaliyetleri üzerinde önemli etkisi olduğu tespit edilmiştir. Söz konusu etki, işletmenin KRY süreçlerinin tamamlanma seviyesi, riskten sorumlu yönetici (CRO) ve denetim komitesinin KRY süreçleriyle ilgili iç denetimden faydalanma isteği, iç denetim yöneticisinin (CAE) görev süresi, işletmenin faaliyet gösterdiği sektör ve iç denetim biriminin KRY'de liderlik rolü üstlenmesi gibi faktörlere bağlıdır (Beasley vd, 2006, s.15-16).

Sarens & Beelde (2006) Amerika ve Belçika menşeili şirketlerde iç denetçilerin risk yönetimi konusundaki mevcut rollerini nasıl algıladıklarını nitel bir araştırmayla ortaya koymayı amaçlamıştır. Çalışmanın sonuçlarına göre Belçika'da iç denetçilerin risk yönetim sistemlerindeki eksikliklere odaklanmaları işletme içindeki değerlerini göstermeleri açısından fırsatlar yaratacaktır. İç denetçiler, risk ve kontrol bilincinin oluşturulması ve risk yönetimi sisteminin oluşturulmasında öncü rol oynamaktadır.

Fraser & Henry (2007) tarafından İngiltere'de yapılan araştırmanın sonuçlarına göre, iç denetimin KRY süreçlerine yüksek seviyede katılım sağlayabileceği keşfedilmiştir. Çalışma kapsamında dört büyük olarak isimlendirilen denetim firmalarının denetçileriyle ve borsada işlem gören beş büyük şirketin finanstan sorumlu yöneticileri (CFO), denetim komitesi başkanları, iç denetçileri ve risk yöneticileriyle görüşmeler yapılmıştır. Çalışmada iç denetçilerin, COSO Risk Çerçevesi ve IIA İç Denetçilerin Risk Yönetimi Rolleri Raporuna göre yönetimde kalması gereken sorumlulukların önemli bir bölümünü de üstlendiği belirlenmiştir. Çalışmanın sonuçlarına göre, birçok durumda IIA'nın KRY konusunda iç denetçi için uygun görmediği görevleri üstlenmesi sonucunda objektifliğini kaybetme riskinin yüksek olduğu anlaşılmıştır.

Castanheira vd. (2010) yaptığı çalışmada KRY'de iç denetimin rolünü araştırmıştır. Bulgulara IIA Portekiz üyesi 96 iç denetim birim yöneticisine gönderilen anket yardımıyla ulaşılmıştır. İç denetimin KRY sorumluluklarını üstlenme konusunda küçük işletmelerde daha aktif olduğu ve söz konusu sorumlulukların özel sektörde özellikle de finans gibi riskli sektörlerde daha fazla önem kazandığı anlaşılmıştır.

Shortreed vd. (2011) iç denetimin kurumsal risk yönetimi kapsamında gelecekte üstlenmesi gereken sorumlulukları ortaya çıkarmak amacıyla teorik bir araştırma yapmıştır. Çalışmada özellikle IIA raporları ve risk yönetimi çerçeveleri incelenmiş ve önemli sonuçlara ulaşılmıştır. İç denetim fonksiyonunun odak noktasında, sadece kontrollerin etkinliği değil, risk yönetiminin etkililiği konusunda güvence sağlamak yer

almalıdır. İç denetim, yönetim adına riskleri üstlenmemeli, sadece uygun risk yaklaşımının benimsenmesi ve sonrasında izlenmesi ve gözden geçirilmesinde yönetime yardımcı olmalıdır. İç denetim, daha etkili risk yönetimini desteklemek için sorumluluklarını güncellemelidir.

Zwaan vd. (2011) tarafından yapılan çalışma, Avustralya'da özel ve kamu sektöründe faaliyet gösteren işletmelerde KRY'nin kullanımını ve KRY'de iç denetimin rolünü keşfetmeyi amaçlamıştır. 117 sertifikalı iç denetçiden KRY'nin kullanımı ve iç denetimin rolüne ilişkin betimleyici veriler toplanmıştır. Elde edilen sonuçlara göre, işletmelerin önemli bir bölümünün KRY çalışmalarına giriştiği ve denetçilerine IIA raporuyla uyumlu sorumluluklar yüklediği anlaşılmıştır. Sonuçlar daha önce yapılan çalışmalarla (Gramling & Myers, 2006) karşılaştırılmıştır.

### 4.1.3. İç Denetimin Uygunluk Sorumlulukları

İç denetimin uygunluk rolü, küreselleşen dünyada uluslararası düzenlemelerin etkisini eskisinden daha fazla hisseden işletmelerin daha fazla uygunluk çabalarına ihtiyaç duymasıyla artmıştır. Dünya ekonomik sistemine entegre olmayı amaçlayan -özellikle gelişmekte olan- ülkelerin yasal düzenlemeler getirmesi veya mevcut düzenlemelerini güncellemesi, işletmelerin uygunluk çabalarını zorunluluk haline getirmiştir. Ayrıca yasal düzenlemelerin yanında işletmenin kendi politika, yordam, strateji ve kodlarına uyum göstermesi; işletme performansı açısından olmazsa olmazdır. İç kontrolün geliştirilmesi sürecindeki görev ve sorumlulukları standartlar, mesleki raporlar ve tanımlar ile vurgulanan iç denetim, iç kontrol ortamının yasa ve düzenlemelere makul güvence sağlaması için çalışmalar yürütür. İç denetimin uygunluk sorumlulukları özellikle Uluslararası Mesleki Uygulama Çerçevesi, İç Denetim Standartları, IIA Raporları ve COSO gibi iç kontrol kapsamında çalışmalar yapan kuruluşların yayınlarıyla belirlenmiş ve araştırmacıların teorik çalışmalarında (Silverman, 2008; Steinberg, 2011; Pickett, 2011; Moeller, 2011; Graham, 2015) vurgulanmıştır.

Özellikle üç hatlı savunma modelinin ikinci hattında bulunan uygunluk fonksiyonunun görev ve sorumluluklarının iç denetimin uygunluk kapsamındaki görev ve sorumluluklarıyla uyumlaştırılması ve iki fonksiyonun yetki alanlarının belirlenmesi ve koordinasyonu önemli bir çalışma alanıdır. Ayrıca iç denetim, işletmenin risk

değerlendirme süreçlerinin bir parçası olarak uygunluk riskini göz önünde bulundurmalı ve denetim planını bu doğrultuda şekillendirmelidir (IIA-UK, 2017, s.1).

Milroy (1995) uygunluk ve iç denetim fonksiyonlarının potansiyel sorumluluk alanlarını teorik olarak incelemiş ve işbirliği yapabilecekleri konuları belirlemeyi amaçlamıştır. İki fonksiyonun amaçları, kapsamı, çalışan nitelikleri ve raporlama kanalları değerlendirilmiştir. Buna göre, iki fonksiyon birçok ortak özelliğe sahip olmasına karşın, ayrı tutulması gereken görevler belirlenmeli ve sorumluluklar ayrılmalıdır. Ancak yine de, ortak görevler konusunda işbirliği yapılmalı ve gereksiz eylemlerin önüne geçilmelidir.

Ruppert (2006) uygunluk çalışanları ve iç denetçiler ile odak grup çalışması yaparak, iki fonksiyonun görev ve sorumluluklarını belirlemeyi amaçlamıştır. Faaliyetler, izleme süreçleri, uygunluk riskleri ve bilgi teknolojileri konularında iç denetçilerin ve uygunluk çalışanlarının görev, yetki ve sorumlulukları karşılaştırılmıştır. Ayrıca iki fonksiyon raporlama kanalları, yönetim kurulu ve üst yönetimle ilişkiler, mesleki standartlar ve amaçlar açısından incelenmiştir. İki fonksiyonun birbirinden farklı rol ve sorumlulukları olduğu gibi benzer rol ve sorumluluklara sahip oldukları da belirlenmiştir. Üstelik bunlar işletmeden işletmeye farklılık gösterir ve kimi durumda birleştirilmiştir. İki fonksiyonun ortak çalışma alanları, yetkileri ve sorumlulukları ortaya çıkarılmalı ve koordinasyon halinde çalışmalar yaparak gereksiz çabaların önüne geçilmeli, uygun raporlar hazırlanmalı ve üst yönetimle ilişkiler düzenlenmelidir.

Thomson Reuters Accelus (2012) raporunda, iç denetim ve uygunluk fonksiyonlarının birbiriyle bağlantılı rolleri incelenmiş ve YRU yaklaşımının temelinde söz konusu ilişkilerin yer aldığı vurgulanmıştır. Üst yönetim ve yönetim kuruluyla ilişkiler, risk yönetimi süreçleri ve izleme yordamları iki fonksiyonun ilişki geliştirebileceği alanlar olarak sıralanmıştır. İki fonksiyonun sorumluluk sınırlarının belirlenmesi ve uygun seviyede işbirliğine gidilmesi gerektiği sonucuna varılmıştır.

### 4.1.4. İç Denetimin Bilgi Teknolojileri Sorumlulukları

Uluslararası İç Denetim Enstitüsü (IIA) 1941 yılında Amerika'da az sayıdaki iç denetçi tarafından kurulduğundan beri, iç denetimin kapsamı ve sorumlulukları çağın gerekleri ölçüsünde gelişim göstermiştir. 1941 yılında meslek resmiyet kazandığında sadece günlük defter kayıtlarının veya hesap işlemlerinin doğru yapılması ve işletmenin şubelerinde işlerin gerektiği şekilde yapıldığıyla ilgilenen iç denetçiler, değişen işletme çevresinde birçok yeni sorumluluğu işlerinin kapsamına almak zorunda kaldılar. İşletme ihtiyaçları ve çevresindeki değişimle şekillenen bu yeni sorumlulukların başında teknolojik yeniliklerin ve işletmenin teknolojiyle değişime uğrayan iş süreçlerinin ve işletmenin kullandığı veya kullanması gereken araçların anlaşılması gelir.

Yeni teknolojiler dünyayı hızla değiştirmektedir. IBM'nin 2012 Küresel CEO Araştırmasına göre, 2004 yılından bu yana, teknoloji ilk kez işletmeyi etkileyen dış faktörler listesinin başında yer almıştır. İşletme yöneticileri, diğer dış faktörlerin hatta ekonominin bile ötesinde, işletmelerinde en fazla teknolojinin değişime yol açmasını beklemektedir (IBM, 2016). Artık iç denetimin görev alanı içerisinde yer alan faaliyetler, bilgi teknolojileri ortamında yürütülmektedir ve iç denetçinin teknolojiyi göz ardı etmesi mümkün değildir. Günümüz işletmelerinde iç kontrol, bilgi teknolojileri ortamında yürütülmektedir ve iç denetim mesleği teknolojik gelişmeleri yakından takip etmek zorundadır. İç denetimin teknolojiyle ilişkisi ve yeni sorumlulukların ne olması gerektiği, IIA'nın mesleği geliştirmek ve yönlendirmek amacıyla hazırladığı rehberler, standartlar ve raporlar ile düzenlenmiştir. Ayrıca akademisyenler tarafından yapılan birçok teorik çalışma (Chorafas, 2001; Moeller, 2004; Moeller, 2009; Pickett, 2011), teknolojinin iç denetim mesleğine etkisine değinmiştir.

IIA'nın yayımladığı 'Bir Adım Öteye Geçmek-İç Denetimde Teknoloji Kullanımı' isimli anket serilerinden oluşan raporunda, iç denetim-teknoloji ilişkisi ve mevcut durum sunulmuştur. Elde edilen verilere göre, iç denetim sürecinde teknoloji kullanımı giderek artmaktadır ancak yine de geliştirilmesi gereken alanlar vardır. BT yazılımları, özellikle sayısal veri analizi tablolarının oluşturulması ve çalışma kâğıtlarının hazırlanması süreçlerini elektronik ortama taşıyarak iç denetimin verimliliğini arttırmıştır. Veri madenciliği ve veri sorgulama araçları, veriye daha kolay erişimi sağlayarak iç denetim faaliyetlerini kolaylaştırmıştır (Cangemi, 2015). Çalışma sonuçlarına göre, dünyanın farklı bölgelerinde ankete katılan iç denetçilerin teknolojiyi kullanma oranı yüzde 27-50 arasında değişmektedir. Elektronik çalışma kâğıtları, otomatik izleme ve denetim izi

sürme araçları, bilgi toplama süreçlerini yönetmek amacıyla kullanılan araçlar ve otomatik veri analitiği araçları iç denetçiler tarafından en fazla kullanılan BT teknikleri ve araçları olmuştur (Cangemi, 2016, s.5).

Rezaee & Reinstein (1998) gelişen bilgi teknolojilerinin denetim fonksiyonu üzerindeki etkisini incelemiştir. Çalışma, işletmelerin bilgi sistemlerinin denetiminde yeterli kanıt toplamak konusunda denetçilere rehberlik eden SAS 80'nin üzerinden bilgi teknolojilerinin etkisini araştırmıştır. İç denetçinin bilgi teknolojilerinde yaşanan hızlı değişimin ve gelişen teknolojik araçların, işletme bilgi sistemi ve denetim yordamları üzerindeki etkisine ayak uydurması gerektiği sonucuna ulaşılmıştır. Gün geçtikçe karmaşıklaşan intranet ve extranet sorunlarının çözümünde iç denetim önemli rol oynamalıdır.

Hermanson vd. (2000) ABD'de faaliyet gösteren işletmelerde BT ile ilgili faaliyetleri incelemek üzere 100'den fazla iç denetçi üzerinde bir araştırma çalışması yürütmüştür. İç denetimin öncelikli olarak BT varlıklarının korunması, veri işleme ve güvenlik gibi geleneksel BT risklerine ve kontrollerine odaklandığı belirlenmiştir. Buna karşın sistem satın alma ve geliştirme gibi alanlar iç denetim birimleri tarafından daha az ilgi görmüştür.

Bierstaker vd. (2001) çalışmasında, teknolojinin iç denetim sürecindeki mevcut etkisini değerlendirmeyi ve teknolojik eğilimlerin denetim mesleği için gelecekteki etkilerini tartışmayı amaçlamıştır. Teknolojinin denetim planına, testlerine ve belgelendirmeye etkisine ilişkin gözlemler tartışılmıştır. Teknolojinin denetim sürecinin neredeyse her aşamasında önemli bir etkiye sahip olmaya devam edeceği sonucuna ulaşılmıştır. İç denetçilerin işletmenin iş süreçlerini kontrol altına alması ve verilerini test etmesi için teknolojiyi anlaması ve ondan faydalanması şarttır. Teknolojinin kullanılması, denetimin etkinliği ve verimliliğinde önemli kazançlar sağlayacaktır.

Rishel & Ivancevich (2003) BT uygulama sürecinde iç denetimin sorumluluklarını tartışmıştır. İç denetimin temel sorumluluğunun, BT uygulamalarının ayrılmaz bir parçası olmak yerine, BT projelerinde özellikle uygulama öncesinde ve izleme aşamasında risk yönetimi sorunlarına ve kontrollere odaklanmak olduğunu savunmuşlardır. Çalışma, iç denetimin BT ortamında uygun kontrollerin geliştirilmesi için çaba göstermesi gerektiğini savunur. İç denetim, yeni sistemlerin ve mevcut sistemlerde yapılan değişikliklerin yeterince belgelenmesini sağlamak için BT ekibi ile iletişim kurmalıdır.

Uygun belgelendirme risk yönetimi ve denetim faaliyetlerinde hayati önem taşıyabileceği için bilgi sistemlerindeki değişikliklerin izlenmesi ve belgelendirilmesini sağlanmalıdır.

Abu-Musa (2008) çalışmasında gelişen bilgi teknolojilerinin iç denetim faaliyetleri üzerindeki etkisini deneysel olarak araştırmış ve elde edilen bulguların farklı özelliklere sahip Suudi işletmelerinde farklılık gösterip göstermediğini incelemiştir. Bu amaçla beş büyük Suudi şehrinde işletmelere gönderilen ankete 281 geçerli dönüş yapılmıştır. Çalışma sonucunda elde edilen verilere göre, iç denetim BT konusunda bilgi ve becerilerini geliştirmelidir. Çalışma sonuçlarına göre, iç denetimin veri gizliliği ve güvenliği, BT varlıklarının korunması ve BT risk yönetimi ve kontrollerinin geliştirilmesi süreçlerine öncelik verdiği anlaşılmıştır. BT ortamında iç denetim performansının; işletmenin faaliyet gösterdiği sektöre, çalışan BT personelinin sayısına ve yeni teknolojilerin kullanılmasına bağlı olduğu anlaşılmıştır.

Teknolojik yazılımların, araçların ve testlerin giderek daha fazla alanda kullanılmaya başlanması, iç denetçiye bir takım sorumluluklar getirmiştir. Söz konusu sorumluluklar, denetim işinde kullandığı teknolojilerin getirdiği sorumlulukların yanında, işletmenin iş süreçlerinde kullanmayı amaçladığı teknolojilerin kurulumu, işletmeye adaptasyonu ve gerektiğinde güncellenmesi süreçlerini kapsamaktadır. Son yıllarda işletme dünyasında adından sıkça söz edilmeye başlanan, işletmenin iç kontrolünü güçlendiren ve iç denetime denetim işinde birçok faydalar sunan YRU yazılımları da bu kapsamdadır. İç denetçiler, YRU yazılımlarının seçimi ve kurulumu sürecinde teknoloji satıcıları ve danışmanlarını anlayabilecek ve gerektiğinde onları ve işletme çalışanlarını yönlendirebilecek seviyede anlayışa sahip olmalıdır. Teknoloji satıcıları ve danışmanların satmaya çalıştıkları ürünler ve tekliflerinin değerlendirilmesi sürecinde iç denetim önemli görevler üstlenir. YRU yazılımları, iç denetim birimlerinin odaklanması gereken bir konu haline gelmiştir (Marks, 2010, s.25).

Marks (2013) çalışmasında, işletmelerin bilgi teknolojilerinden yararlanma çabası içine girmesinin, iç denetim birimlerine etkinlik ve verimliliklerini artırmak amacıyla kurumsal uygulamalara katılma noktasında büyük fırsatlar sunduğunu savunmuştur. İşletmeler, ürün teslim etme veya müşterilerle iletişim kurma biçimlerini değiştirme gibi faaliyetlerin yanında işletmenin yönetilmesini kolaylaştıran çeşitli teknolojilere yatırım yapmaktadır. Çalışma sonuçlarına göre, denetçiler, iç denetim çalışmalarını dönüştürmek amacıyla bu araçlardan faydalanmalıdır. Riskin değerlenmesi ve izlenmesi, denetim faaliyetlerinin yönetilmesi, denetim testlerinin yapılması, denetimin raporlanması ve

iletişim kanallarının geliştirilmesi alanlarında bilgi teknolojilerinin, iç denetçilere hem faydalar sağladığı hem de sorumluluklar yüklediği savunulmuştur.

KPMG (2017) iç denetçilere daha faydalı teknolojik ürünler sunulabilmesi amacıyla, işletme ihtiyaçlarının yönlendirdiği iç denetim faaliyetlerine yönelik olarak, teknoloji çözümlerinin en fazla odaklanması gereken alanları belirlemeye çalışmıştır. Çalışma sonuçları, iç denetimin teknolojiden mevcut beklentilerini yansıtması açısından önemlidir. İç denetimin teknolojiden çözüm beklediği konular; siber güvenlik, birleşme-devralma-bölünme işlemleri, veri analitiği, veri yönetimi, sistem uygulama ve güncelleme, yeni muhasebe standartları, küresel uygunluk çerçevesi, araştırma-geliştirme verimliliği olarak tespit edilmiştir. Teknoloji, bu alanlarda iç denetime birçok fayda sağlayacağı gibi yeni görevler ve sorumluluklar da getirecektir.

### 4.1.5. YRU Yaklaşımının Faydaları

OCEG dünyanın farklı coğrafi kesimlerinden büyük işletmelerden oluşan örneklemler üzerinde birçok çalışma yapmıştır. Bu çalışmalarda YRU Yaklaşımının sağladığı faydalar değerlendirilmiştir. İşletmelerin YRU yaklaşımından elde edeceği faydalar, danışmanlık firmaları (PWC, KPMG, EY, Deloitte, gibi) ve teknoloji sağlayıcılarının (Gartner, SAP, MetricStream, IBM, Microsoft, Oracle, Workiva gibi) raporlarında ve işletmelerin farklı alanlarda gelişmesi amacıyla çalışan kar amacı gütmeyen kuruluşların (IIA, COSO, ISACA, PMI, OCEG gibi) rehber ve çerçevelerinde kendisine yer bulmuştur.

OCEG yöneticisi Carole Switzer, işletmelerin yönetişim-risk-uygunluk faaliyetleri ve ilişkili diğer faaliyetlerine YRU yaklaşımının sağladığı ortak bakış açısının; risk yönetimini amaçlarla uyumlu hale getirme, karmaşıklığı azaltma, tutarsızlıkları azaltma ve teknolojiyi en uygun şekilde kullanma gibi faydalar sağlayacağını savunmaktadır. Switzer'e göre, YRU yaklaşımı, karar almayı hızlandırır, örgütsel çevikliği geliştirir ve maliyetleri düşürür (IIA, 2010, s.1).

OCEG çerçevelerinde (OCEG, 2009, 2015), YRU yaklaşımının faydaları incelenmiştir. YRU yaklaşımının işletmede iletişimi geliştireceği, stratejilerin işletme birimleri arasındaki işbirliğiyle geliştirileceği, ortak süreçlerden ve teknoloji çözümlerinden yararlanılacağı vurgulanmıştır. YRU yaklaşımı, farklı işletme birimlerine faaliyetleriyle ilgili çeşitli faydalar sağlamanın yanında genel olarak, gereksiz faaliyetlerin belirlenmesini sağlayarak maliyetleri azaltır; sağladığı bütünleşik yapıyla

hataları ve boşlukları azaltır; stratejik ve taktik kararların risk bilgisiyle alınmasını sağlayarak bilginin kalitesini artırır ve amaçların açıkça ifade edilmesini ve çalışanlarla paylaşılmasını sağlayarak motivasyonu artırır. YRU yaklaşımı, işletmede örgütsel kültürü geliştirir, stratejik planların ve amaçların riskin göz önüne alınarak hazırlanmasını sağlar, paydaşların güvenini arttırır, zayıf veya sorunlu alanların keşfedilmesini ve ortadan kaldırılmasını sağlar.

OCEG (2015), işletmenin çalışanları, süreçleri ve kullandığı bilgi teknolojilerini geliştirerek risk yönetimi, yönetişim ve uygunluk çabalarında başarıya ulaşmasını destekleyen YRU yaklaşımının başlıca faydalarını;

- Paydaşların beklentilerini anlamak,
- İşletmenin riskleri ve değerlerine uygun olarak amaçlarını düzenlemek,
- İşletme amaçlarına en uygun risk profilinin benimsenmesi ve işletme varlıklarının korunmasını sağlamak,
- Sözleşmeler ve yasal düzenlemeler, işletme politikaları, sosyal normlar ve etik ilkelerden oluşan sınırlar içerisinde faaliyet göstermek,
- Paydaşlara ilgili, güvenilir ve zamanında bilgi sunmak,
- İşletmenin sistem performansının ve etkinliğinin ölçülmesini sağlamak olarak sıralamıştır.

Garsoux & Soenen (2017) hazırladıkları ISACA raporunda, YRU yaklaşımının üç hatlı savunma modeliyle ilişkisini incelemiştir. Rapora göre, YRU yaklaşımı, gereksiz faaliyetleri ortadan kaldırarak maliyetleri azaltır, bütüncül risk ve kontrol çerçevesiyle riskli olayların etkisini azaltır, risk ve kontrol eylem planlarının daha tutarlı hazırlanmasını sağlar, kıt kaynakların en uygun şekilde kullanılmasını sağlar ve stratejik planların hazırlanması için gereken risk tabanlı bilginin kalitesini arttırır.

KPMG (2014) yayımladığı raporda, YRU yaklaşımının sağladığı ortak dilin risk ve kontrol süreçlerinde verimliliği artırdığını, yasal gereksinimlere uygunluğu sağlayarak değişikliklere karşı esnekliği geliştirdiğini ve uygunluk, risk yönetimi, denetim ve diğer güvence birimlerinde hataları önlediğini belirlemiştir. Ayrıca YRU yaklaşımı, denetim ve risk yönetimi faaliyetlerinde maliyetleri azaltır ve işletmede raporlama faaliyetlerinin kalitesini artırır.

Madlener (2009) yaptığı çalışmada, uzman görüşleri ile YRU yaklaşımının işletme bilgi sistemlerine etkisini ortaya çıkarmak amacıyla delphi tekniğini kullanmıştır. YRU yaklaşımının işletmenin yönetişim, risk yönetimi ve uygunluk süreçlerine

sürdürülebilirlik, verimlilik, şeffaflık ve tutarlılık getirebileceğini vurgulanmıştır. YRU yaklaşımının faydalarına ancak ilgili çalışanlar arasında işbirliği ve ortak teknoloji altyapısı geliştirilerek ulaşılabileceği ve YRU'nun işletmenin iç kontrol yapısına değer katan bir yaklaşım olduğu sonucuna ulaşılmıştır.

### 4.2. Araştırmanın Yöntemi

Araştırma kapsamında iç denetimin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini ölçmek amacıyla iç denetim kuramı, mevcut literatür ve uzman görüşlerinden yola çıkılarak geliştirilen hipotezlerin test edilmesi için Yapısal Eşitlik Modeli (YEM) geliştirilmiştir. YEM, regresyon analiziyle benzerlikler göstermesine karşın, kuramsal yapılar arasındaki ilişkilerin modellenmesine ölçme hatalarının ve hatalar arası ilişkilerin dahil edilmesini mümkün kılan çok değişkenli istatistiksel bir tekniktir. YEM, araştırma modeline gömülü olan hipotezlerin içinde yer alan yapılar arasındaki sebep-sonuç ilişkilerini açıklayabilen ve geliştirilen modellerin bir bütün halinde test edilmesini sağlayan bir model geliştirme ve değerlendirme yöntemidir (Raykov & Marcoulides, 2006).

YEM'de ilişkilerin gösterilmesinde çoğu zaman path (yol) analizi ve diyagramından yararlanılır. Path sözcüğünün dilimizdeki anlamı 'yol' veya 'rota'dır. Anlamına uygun şekilde yol analizi, bağımlı (içsel) yapıların ya da değişkenlerin bağımsız (dışsal) yapılarla ya da değişkenlerle bağlantısını belirleyen ilişki yollarının geliştirilmesini sağlayarak, bir ya da birden fazla regresyon denkleminin elde edilmesine fırsat tanır. Modelde yapılar arası ilişkiler tek yönlü (nedensel) olabileceği gibi çift yönlü (korelasyonel) de olabilir (Arı & Yılmaz, 2015, s. 124).

YEM gözlenen ve gözlenemeyen (örtük ya da gizil) değişkenler arasındaki örüntülerin sınanmasında kullanılır. Sosyoloji, pazarlama, ekonometri, psikoloji ve eğitim bilimlerinde yapılar arasındaki ilişkilerin test edilmesinde ve literatürde yer alan veya literatür destekli geliştirilen kuramsal modellerin sınanmasında kullanılır. YEM, örtük (gözlenemeyen ya da gizil) değişkenlerin gözlenen değişkenler aracılığıyla ölçülebileceği ve örtük değişkenler arasında nedensellik ilişkisi olduğu varsayımlarına dayanır. Gözlenemeyen değişkenlerin ölçülebilmesi, ancak gözlenen değişkenler ile ilişki kurularak mümkün hale gelir. Araştırmacının, gözlenemeyen değişkenleri, öngörülen yapı açısından işlemsel olarak tanımlamak amacıyla, gözlenebilir değişkenlerle ilişkilendirmesi bir zorunluluktur (Yılmaz, Çelik & Ekiz, 2006, s. 175).

YEM, öngörülen bir modelde yer alan değişkenlerin doğrudan ve dolaylı etkilerinin birlikte ele alınmasını ve ölçme hatalarının modele dâhil edilmesini sağlayarak, çok değişkenli modellerin tahmin edilmesini, geliştirilmesini ve test edilmesini sağlar. Geleneksel regresyon modellerinin tersine YEM'de açıklayıcı değişkenlerin ölçme hataları, etkin şekilde önemsenir. YEM'in uygulama aşamaları sırasıyla, (1) kuramsal modelin geliştirilmesi, (2) geliştirilen modelde yer alan ilişki örüntülerini gösteren yol diyagramının çizilmesi, (3) yol diyagramıyla ölçüm ve yapısal modellerin ayrıştırılması, (4) önerilen modelin tahminlerinin elde edilmesi, (5) modelin uygunluğunun değerlendirilmesi ve sonuçların yorumlanmasıdır (Çelik & Yılmaz, 2013, s. 8).

YEM; regresyon analizi, faktör analizi ve varyans (kovaryans) analizi gibi çok sayıda analiz yöntemini kapsayan bir modelleme zinciridir (Byrne, 2011, s.12). Ölçüm modeli ve yapısal model olmak üzere iki alt modelden oluşur. Ölçüm modeli, gözlenemeyen değişkenlerin gözlenen değişkenler aracılığıyla ne kadar iyi ölçüldüğünün değerlendirildiği ve doğrulandığı modeldir. Ölçüm modelleri Doğrulayıcı Faktör Analizi'nin (DFA) en yalın halidir. Yapısal model test edilmeden önce, DFA yürütülmeli ve ölçüm modelleri doğrulanmalıdır. Yapısal model ise, çalışılan konu hakkındaki hipotetik ilişkilerin test edildiği aşamadır. Yapısal modelde bağımsız (dışsal) değişkenlerin bağımlı (içsel) değişkenleri açıklama oranı ortaya çıkarılır (Aksu, Eser & Güzeller, 2017, s. 61).

Araştırmamızda ölçüm modeli ve yapısal model aşamalarına geçilmeden önce, veri toplama aracıyla elde ettiğimiz veri setimizdeki yapıların (faktörlerin) ortaya çıkarılması amacıyla, Açımlayıcı Faktör Analizi (AFA) yürütülmüştür. AFA, veri setindeki yapıların sayısı hakkında net bir bilgiye sahip olunmadığı zaman, bir hipotezi test etmek yerine önsel olarak kurgulanan yapıların (istatistik terminolojisiyle faktörlerin) sayısı ve özelliklerinin belirlenmesi amacıyla başvurulan bir tekniktir. Çalışmamızda iç denetimin sorumluluklarına ve YRU yaklaşımının faydalarına ilişkin yapıların keşfedilmesi için AFA uygulanmıştır.

Ölçüm modeli ve yapısal modelden oluşan süreç sonunda üzerinde çalışılan konu hakkındaki hipotetik veya anlamlı bilginin bir model aracılığıyla ortaya konulması sağlanır. Araştırmamız kapsamında öncelikle iç denetimin sorumluluklarına ve YRU yaklaşımının faydalarına ilişkin AFA ile keşfedilen faktör yapılarını betimleyen ölçüm modelleri, DFA uygulanarak değerlendirilmiştir. Daha sonra, iç denetimin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini test etmek amacıyla

geliştirilen hipotezler, yapısal model aracılığıyla ortaya konulmuş ve değerlendirilmiştir. Analizler LISREL 9.1 programı ile yürütülmüştür.

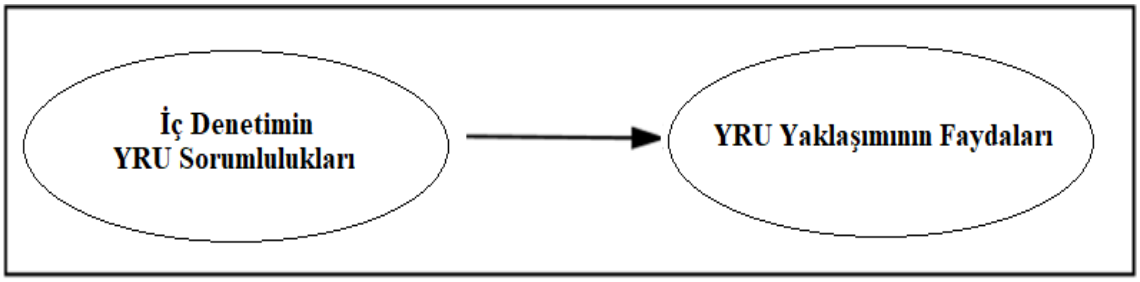
Araştırmamız kapsamında iç denetçilerin sorumlulukları ve YRU yaklaşımının faydaları ile ilgili iç denetçilerden oluşan katılımcı grubu ile bağımsız denetçiler ve işletme yöneticilerinden oluşan grubun görüşlerini karşılaştırmak amacıyla bağımsız örneklemler t testleri yürütülmüştür. Ayrıca iç denetçilerin ve diğer katılımcıların olması gereken durum ve uygulamadaki duruma ilişkin görüşlerini karşılaştırmak amacıyla ayrı ayrı eşleştirilmiş örneklemler t testleri yürütülmüştür. Söz konusu analizlerin yürütülmesinde AFA ile keşfedilen yapılar (faktörler) kullanılmıştır. Böylece iki grubun görüşleri arasında ya da olması gereken ve uygulamadaki duruma yönelik görüşler arasında farklılıklar ayrıntılı olarak ortaya konulabilmiştir.

T testleri, iki grup ya da iki durum için sürekli değişkenlerden elde edilen değerlerin karşılaştırılmasını sağlar. İki farklı grubun ya da iki farklı durumun ortalamalarını karşılaştırmak istediğimizde bağımsız örneklemler t testlerini kullanırız. Faklı grupların yanıtlarını karşılaştırmak istediğimizde, uygulayacağımız parametrik test, bağımsız örneklemler t testidir. Eğer iki farklı durumda aynı grupta yer alan kişilerden ya da eşleştirilmiş çiftlerden elde ettiğimiz ortalama değerleri karşılaştırmak istiyorsak eşleştirilmiş örneklemler t testlerini kullanırız. Aynı grubun iki farklı soruya verdiği yanıtları karşılaştırmak istediğimiz zaman, uygulayacağımız parametrik test, eşleştirilmiş örneklemler t testi olmalıdır.

İç denetçilerden oluşan grup ile bağımsız denetçiler ve işletme yöneticilerinden oluşan grubun, iç denetçilerin sorumluluklarına ve YRU yaklaşımının faydalarına ilişkin AFA sonucunda keşfedilen ve isimlendirilen yapılar hakkında olması gereken ve uygulamaya yönelik görüşlerinin ortalamaları eşleştirilmiş örneklemler t testleri ile ayrı ayrı analiz edilmiştir. Eşleştirilmiş örneklemler t testi, ilişkili iki örneklem ortalaması arasındaki farkın anlamlı olup olmadığını değerlendirmek için uygulanır. Grupların görüşleri arasındaki farklılıklar ise, bağımsız örneklemler t testleriyle analiz edilmiştir. Bağımsız örneklemler t testi, ilişkisiz iki örneklemin ortalamaları arasındaki farkın anlamlı olup olmadığını test eder. Betimsel ve yordayıcı analizlerde, SPSS 24.0 programından faydalanılmıştır.

### 4.2.1. Araştırma Modeli ve Hipotezler

Araştırmamızda iç denetimin YRU yaklaşımı kapsamındaki sorumluluklarının YRU Yaklaşımının sağladığı faydalar üzerindeki etkisini incelemek üzere, ilişkisel tarama (kesitsel) metodu uygulanmıştır. Karasar (2011, s. 81), ilişkisel tarama metodunu, "iki veya ikiden fazla değişken arasında birlikte değişimin varlığını ve/veya ölçüsünü belirlemeyi amaçlayan araştırma modelleri" olarak ifade etmiştir. Değişkenlere müdahale etmeden aralarındaki ilişkiyi istatistiksel tekniklerle araştırmaya çalışan bu modelde, değişkenler keşfedici ya da yordayıcı olabilmektedir. Yordayıcı değişkenin araştırılmasında amaç, değişkenler arasında anlamlı bir ilişki saptamakken; keşfedici değişkenin araştırılma amacı, bağımlı değişkeni etkileyen nedenleri belirlemektir (Sönmez ve Alacapınar, 2014, s. 50). Araştırmanın temel modeli Şekil 4.1'de verilmiştir.

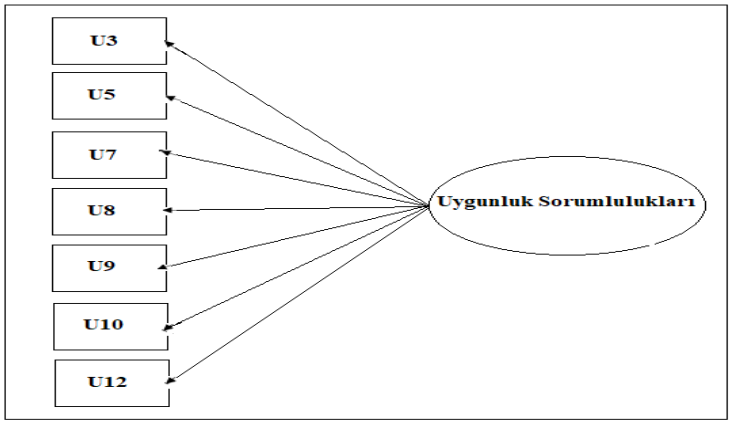



**Şekil 4.1.** *Araştırmanın Temel Modeli*

Araştırmanın amacı, YRU kapsamında iç denetim sorumluluklarının YRU yaklaşımından beklenen faydalar üzerinde anlamlı bir etkisinin olup olmadığının incelenmesidir. Bu ilişkinin varlığını ortaya çıkarmak ve hangi sorumlulukların etkisinin olduğunu keşfetmek amacıyla, iç denetimin sorumluluklarının alt boyutları değerlendirilmiştir.

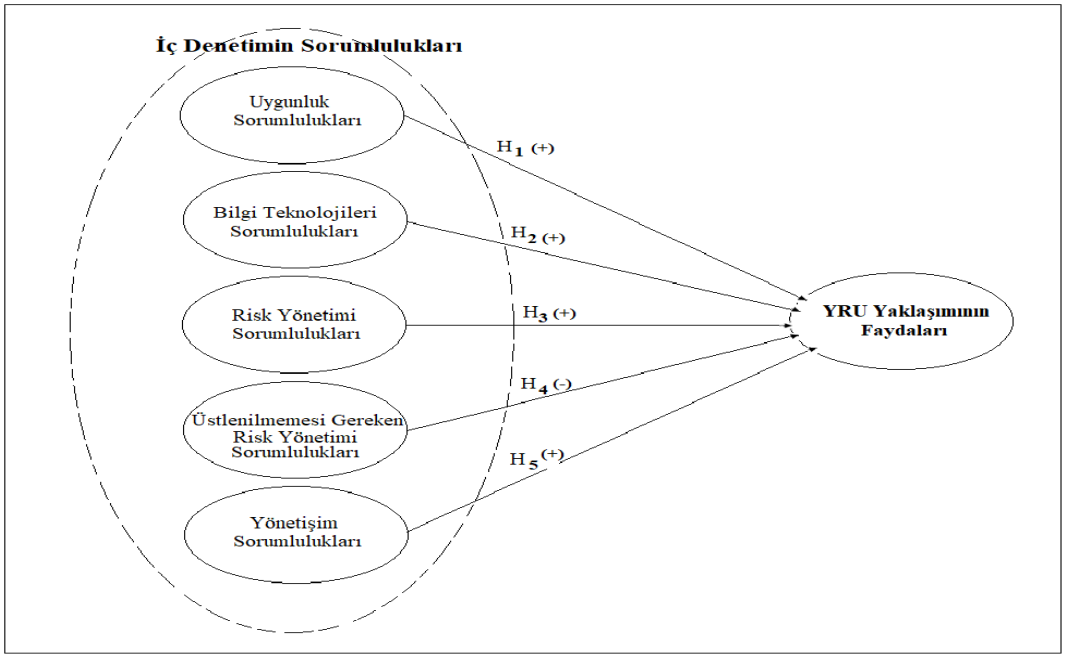
Araştırma modelinin test edilmesinde, YEM kullanılmıştır. YEM, gözlenen ve gizil değişkenler arasındaki ilişkilerin keşfedilmesini ve ölçülebilmesini sağlayan güçlü bir istatistiksel tekniktir. YEM'de örneklemden direk olarak gözlemlenen veya gözlenebilme olanağına sahip değişkenler olarak tanımlanan ve araştırmamız kapsamında veri derleme aracındaki ölçek maddelerinin her biri olarak somutlaştırdığımız gözlenen değişkenler dörtgenle gösterilir. Doğrudan gözlenemeyen veya ölçülemeyen değişkenler olarak tanımlanan ve araştırmamızda aralarında ilişki keşfetmeye çalıştığımız iç denetimin sorumlulukları ve YRU yaklaşımının faydaları olarak somutlaştırdığımız gizil (örtük) değişkenler ise, elipsle gösterilir. Örnek olarak, iç denetimin uygunluk sorumlulukları

gizil değişkeni ve veri toplama aracımızda söz konusu gizil değişkenin ölçülebilmesini sağlayan gözlenen değişkenlerin gösterimi, Şekil 4.2'de verilmiştir.




**Şekil 4.2.** *Uygunluk Gizil Değişkeni ve Gözlenen Değişkenler*

Araştırmamızda öngörülen model Şekil 4.3'te sunulmuştur. Görüldüğü üzere, öngörülen model altı gizil değişkene sahiptir. Gizil değişkenler veri derleme aracında yer alan gözlenen değişkenler aracılığıyla ölçülmüştür. İç denetimin YRU yaklaşımı kapsamındaki sorumluluklarına ilişkin beş gizil değişken ve YRU yaklaşımının faydalarına ilişkin bir gizil değişken veri derleme aracındaki önermeler ile somutlaştırılmıştır.




**Şekil 4.3.** *Kavramsal Olarak Önerilen Model*

Çalışmamız kapsamında geliştirilen araştırma modelinden hareketle, test edilmesi amaçlanan hipotezlerimiz şunlardır:

$H_1$= İç denetimin uygunluk sorumlulukları YRU yaklaşımının faydalarını pozitif yönde etkiler.

$H_2$= İç denetimin bilgi teknolojileri sorumlulukları YRU yaklaşımının faydalarını pozitif yönde etkiler.

$H_3$= İç denetimin risk sorumlulukları YRU yaklaşımının faydalarını pozitif yönde etkiler.

$H_4$= İç denetimin üstlenmemesi gereken risk sorumlulukları YRU yaklaşımının faydalarını negatif yönde etkiler.

$H_5$= İç denetimin yönetişim sorumlulukları YRU yaklaşımının faydalarını pozitif yönde etkiler.

Çalışmamız kapsamında iç denetçilerin YRU kapsamında üstlenmeleri gereken sorumlulukları saptayarak uygulamadaki durumla karşılaştırmak ve söz konusu sorumlulukları iç denetim hizmetlerinden doğrudan etkilenen taraflar olarak tanımladığımız işletme yöneticileri ve bağımsız denetçilerin görüşleriyle karşılaştırmak araştırmamızın amaçlarındandır. Ayrıca iç denetçilerin, YRU yaklaşımının faydalarına ilişkin görüşlerini tespit etmek ve iç denetim hizmetlerinden doğrudan etkilenen taraflar olan diğer katılımcıların görüşleriyle karşılaştırmak yine araştırmanın amaçları arasındadır. Mevcut literatür ve araştırma amaçları doğrultusunda test edilmesi amaçlanan ana hipotezler, bağımsız örneklemler t testi ve eşleştirilmiş örneklemler t testleri ile istatistiksel olarak değerlendirilmiştir. Bu hipotezler şunlardır:

$H_6$= İç denetçilerin, iç denetimin sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır. $H_6$ Hipotezinin alt hipotezleri şunlardır:

$H_{6a}$= İç denetçilerin, uygunluk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{6b}$= İç denetçilerin, bilgi teknolojileri sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{6c}$= İç denetçilerin, risk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{6d}$= İç denetçilerin, yönetişim sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{6e}$= İç denetçilerin, üstlenmemesi gereken risk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_7$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır. $H_7$ Hipotezinin alt hipotezleri şunlardır:

$H_{7a}$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin uygunluk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{7b}$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin bilgi teknolojileri sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{7c}$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin risk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{7d}$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin yönetişim sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{7e}$= İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun, iç denetimin üstlenmemesi gereken risk sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_8$= İç denetimin sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun

görüşleri arasında istatistiksel olarak anlamlı farklılık vardır. $H_8$ Hipotezinin alt hipotezleri şunlardır:

$H_{8a}$= İç denetimin uygunluk sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{8b}$= İç denetimin bilgi teknolojileri sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{8c}$= İç denetimin risk sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{8d}$= İç denetimin yönetişim sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{8e}$= İç denetimin üstlenmemesi gereken risk sorumlulukları hakkında olması gereken duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_9$= İç denetimin sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır. $H_9$ Hipotezinin alt hipotezleri şunlardır:

$H_{9a}$= İç denetimin uygunluk sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{9b}$= İç denetimin bilgi teknolojileri sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{9c}$= İç denetimin risk sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{9d}$= İç denetimin yönetişim sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{9e}$= İç denetimin üstlenmemesi gereken risk sorumlulukları hakkında uygulamadaki duruma ilişkin iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

$H_{10}$= YRU yaklaşımının faydaları hakkında iç denetçilerin görüşleri ile bağımsız denetçiler ve işletme yöneticilerinden oluşan grubun görüşleri arasında istatistiksel olarak anlamlı farklılık vardır.

### 4.2.2. Araştırmada Kullanılan Veri Toplama Aracı

Bilimsel araştırma ölçmeye dayanır. Duyarlı ölçüm araçlarıyla yapılan ölçümler bilimsel gelişmeyi arttırır. Ölçülmek istenen özelliklerin sınıflanması, sıralanması veya miktar ve derecelerinin tespit edilmesi amacıyla uyulması gereken kural ve kısıtlamaları belirleyen ölçme araçları ölçek olarak tanımlanır (Karakoç & Dönmez, 2014, s.40). Ölçek geliştirme çalışmasının ilk adımı, ölçmek istenen yapının açıkça belirlenmesi amacıyla literatür incelemesi yapmaktır. Literatür incelemesi yaparken, hangi konuların değerlendirilmeye alınması gerektiği belirlenmelidir (DeVellis, 2003, s.60). Çalışmamız kapsamında ilgili literatür ayrıntılı olarak incelenmiş ve veri toplama aracında çalışmanın kurgusuyla tutarlı konular belirlenmiştir.

Literatür incelemesiyle ölçeğin amacı açık bir biçimde ifade edildikten sonra, ilk adım ölçeğe nihai olarak dahil edilmeye aday geniş bir madde havuzunun oluşturulmasıdır. Ölçüm şekli için Likert tipi formatın kullanılmasına karar verilmiş ve madde havuzu formata uygun olarak hazırlanmıştır. Madde havuzu geliştirilirken, maddelerin sade ve anlaşılır olmasına, birden fazla yargıyı nitelememesine özen gösterilmiştir. Ölçek maddelerinin tanımlanan yapının sınırlarının ötesine geçmemesine özen gösterilmiştir. Çünkü maddeler, çalışılan kavramın yetersiz bir yansıması olursa ya da kavramın sınırlarının ötesine geçerse, ölçek yapının özünü doğru bir biçimde oluşturamaz (DeVellis, 2003, s.64).

Madde havuzu oluşturulurken, ilgili literatürden yararlanılarak çok sayıda ölçek maddesi geliştirilmiştir. Madde havuzu, çalışmanın sonunda bulunan EK-2'de sunulmuştur. Soru ifadelerinin amaçlanan kavramsal çerçeveye ilişkin görüşü ölçme gücü, katılımcılar tarafından aynı şekilde anlaşılabilirliği, kolay okunabilirliği ve ifade uzunluğu tek tek incelenmiştir. Madde havuzundan iki yönlü, çoklu olumsuzlamayla kurgulanmış veya hangi isme ait olduğu anlaşılamayan zamirler içeren ifadeler

düzeltilmiş ya da aynı görüşü ölçtüğü düşünülen ifadeler, veri derleme aracından çıkarılmıştır. Literatür incelemesi sonrasında ölçek maddesi olma nitelikleri taşıdığı düşünülen ifadeler, bir yükseköğretim kurumunda çalışan kamu iç denetçileriyle ve TİDE üyesi iç denetçilerle tartışılmıştır. İfadelerin veri derleme aracına uygunluğunun yanı sıra iyi bir ölçek maddesinin taşıması gereken özelliklere sahip olup olmadığı üzerine yüz yüze görüşmeler yapılmıştır.

Ölçme aracının maddeleri ile ölçülmek istenen özellik arasındaki bağıntı ölçme aracının geçerliliğini ifade eder. Ölçme aracının ölçülmek istenen özelliği kapsama veya sorunun ilgili maddeyi yorma gücü, önsel çalışmalarla belirlenebilir (McGartland vd., 2003). Ölçekteki soruların anlaşılabilir olması veya hedef kitleye uygunluğu ölçeğin geçerliliğini etkileyen diğer faktörler olarak dikkate alınmalıdır. Önsel çalışmalarla elde edilen uzman görüşleri ölçek maddeleri arasındaki uyum geçerliliğini kestirmek için kullanılmaktadır (Yurdugül, 2005, s.771). Bu sebeple ölçme aracının elde edilmesi sürecinde mümkün olduğunca uzman görüşlerinden istifade edilmiştir.

Madde havuzu geliştirildikten sonraki aşama, uzman görüşlerinden faydalanmaktır. Uzmanlar soruların uygunluğu ve anlaşılırlığını değerlendirip, soruların değiştirilmesi ya da çıkarılmasını önerebilirler. Ancak tavsiyelerin dikkate alınması kararı, ölçeği hazırlayanın iradesine bırakılmalıdır. Uzman görüşleriyle kapsam ve görünüş geçerliliği değerlendirilmiş olur (Taşkın ve Akat, 2010, s.20).

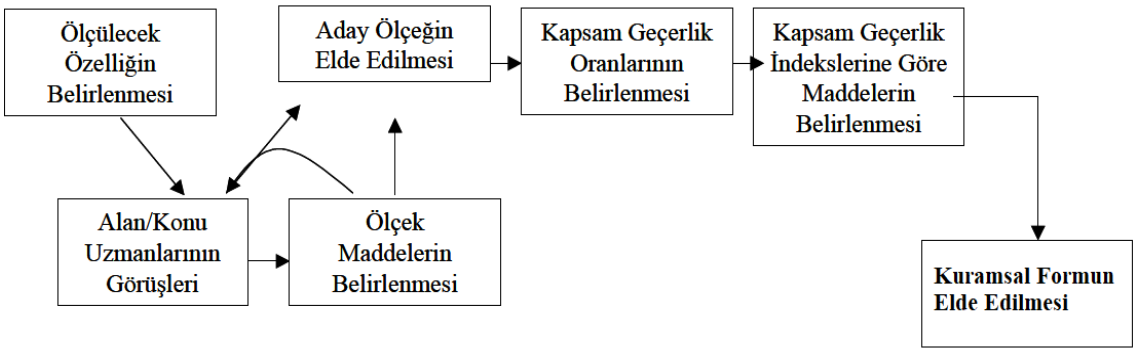
Görünüş geçerliliği ölçme aracındaki maddelerin açık bir şekilde araştırılan konuyla ilgili bilgiye yönelik olduğuna dair uzman görüşüdür. Görünüş geçerliliğinin teknik bir geçerlilik olarak kabul edilemeyeceğini savunanlar vardır (Karakoç ve Dönmez, 2014, s.42).

Kapsam geçerliliği ise, ölçeğin tamamının ya da ölçekteki her bir sorunun/maddenin ölçme aracının amacına ne düzeyde hizmet ettiğidir. Ölçeğin kapsam geçerliliğini sağlamak için uzmanların görüşüne başvurulur. Konuyla ilgili kapsam belirlemesi yargılama yapmayı gerektirdiği için farklı ölçütlere göre değerlendirme yapılmasının önüne geçilmesi amacıyla uzmanlar ile ölçeği geliştiren arasında tanımlar konusunda uzlaşılması gereklidir. Kapsam geçerliliği için yapılan çalışmalar sonucunda ölçek, maddelerin sunum biçiminin yaptığı farklı tepkiler açısından yani görünüş geçerliliği açısından da değerlendirilmiş olur (Tavşancıl, 2002). Çalışmamızda ölçme aracında bulunan her maddenin, anketin amacına ne kadar hizmet ettiğini değerlendirmek için kapsam geçerliliği çalışması yapılmıştır (Dündar vd., 2017, s.198).

Ölçek maddelerinin ölçülmesi amaçlanan özellikleri ölçüp ölçmediğinin belirlenmesi aşamasında, en yaygın kullanılan teknik olan Lawshe (1975) adıyla bilinen çalışma yapılmıştır. Lawshe tekniği, altı adımdan oluşur:

1. Alan uzmanları ekibinin oluşturulması,
2. Aday ölçek formunun hazırlanması,
3. Uzman görüşlerinin alınması,
4. Maddelere ilişkin kapsam geçerlilik oranlarının hesaplanması,
5. Ölçeğin kapsam geçerlilik indeksinin hesaplanması,
6. Kapsam geçerlilik indeksine göre aday ölçek formunun oluşturulması.

Kuramsal ölçek formunun elde edilme süreci Şekil 4.4'te özetlenmiştir.




**Şekil 4.4.** *Kuramsal Formun Elde Edilme Süreci*

Kuramsal form elde edilirken ilk aşamada, araştırma kapsamında ölçülmesi amaçlanan faktörler, araştırma modeline uygun olarak belirlenmiştir. Daha sonra YRU yaklaşımı ve iç denetimi ele alan teorik literatür incelenerek ölçme aracına uygun çok sayıda ölçek maddesi hazırlanmıştır. Ölçek maddeleri araştırmacı tarafından tez danışmanı ile birlikte ifadelerin açıklığı, ölçme aracıyla ilgisi ve dilbilgisi açısından tek tek elemeye tabi tutulmuş ve uygun görülmeyen ölçek maddeleri havuzdan çıkarılmıştır.

Geliştirilen madde havuzu, konuyla ilgili bilgiye sahip olduğu düşünülen 20 kişilik alan uzmanları ekibine sunulmuştur. Ölçülmesi amaçlanan olguya ilişkin geliştirilen her bir madde anlaşılırlık ve ölçme aracına uygunluk açısından alan uzmanları ekibi tarafından değerlendirilmiştir. Böylece ölçekte yer alan ölçek maddelerinin; geliştirilen ölçeğin kalitesini azaltan jargon sözcük, iki yönlü ifade, çoklu olumsuzlama ve hangi ismi nitelediği belirsiz zamirlerden arındırılması sağlanmıştır. Ayrıca okunması zor veya çok uzun maddelerin havuzdan çıkarılması sağlanmıştır.

Lawshe tekniğinde 5 ile 40 arasında uzmanın görüşüne ihtiyaç duyulur. Uzman görüşleri, kapsam geçerliliğinin dışında soruların anlaşılabilirliği ve örnekleme uygunluğu açısından da değerlendirilir. Uzmanların herhangi bir maddeye ilişkin görüşlerinden kapsam geçerlik oranları (KGO) elde edilir. Bir maddenin kapsam geçerlik oranı, olumlu görüş belirten uzman sayısının maddeyle ilgili görüş belirten uzman sayısının yarısına oranının bir eksiğidir (Dündar, 2017, s.198).

$$KGO = \frac{N_G}{N/_2} - 1$$

$N_G$ Maddeyi uygun bulan uzmanların sayısını, $N$ ise maddeye yanıt veren uzmanların sayısını gösterir. KGO'su 0 ya da eksi değer alıyorsa, madde hemen elenir. KGO'su 0'dan büyük maddelerin anlamlılıkları, istatistiksel ölçütlerle test edilir. $\alpha$=0.05 anlamlılık düzeyinde kabul edilebilir en düşük değerler, Veneziano & Hooper (1997) tarafından tablo haline getirilmiştir (Bkz. Tablo 4.1). Uzman sayısına göre en düşük değerler aynı zamanda maddenin istatistiksel olarak anlamlılığını verir. KGO kritik sınırının altında kalan maddeler ölçekten çıkarıldıktan sonra kalan maddelerin KGO değerlerinin aritmetik ortalaması, kapsam geçerlik indeksini (KGİ) verir (Dündar, 2017, s.199).

**Tablo 4.1.** *Katılımcı sayısına göre kritik KGO değerleri (p=0,05)*

| Uzman Sayısı | Min. Değer | Uzman Sayısı | Min. Değer |
|---|---|---|---|
| 5 | 0,99 | 13 | 0,54 |
| 6 | 0,99 | 14 | 0,51 |
| 7 | 0,99 | 15 | 0,49 |
| 8 | 0,78 | **20** | **0,42*** |
| 9 | 0,75 | 25 | 0,37 |
| 10 | 0,62 | 30 | 0,33 |
| 11 | 0,59 | 35 | 0,31 |
| 12 | 0,56 | 40+ | 0,29 |

*Mevcut çalışma için kritik sınır değeri

Araştırma kapsamında iç denetçilerin sorumluluklarını belirlemek amacıyla düzenlenen madde havuzunda 91 ölçek maddesi, YRU yaklaşımının faydalarını tespit etmek amacıyla düzenlenen madde havuzunda 24 ölçek maddesine yer verilmiştir. Araştırmada 20 alan uzmanının görüşlerinden faydalandığı için 0,42 çalışmanın KGO kritik sınır değeridir. Tüm ölçek maddeleri için KGO değerleri hesaplandıktan sonra KGO değerleri kritik eşiğin (0,42) altında kalan maddeler ölçekten çıkarılmış, kalan

maddelerin KGO değerlerinin aritmetik ortalaması iki ayrı madde havuzunun KGİ'sini vermiştir (Bkz. Tablo 4.2, Tablo 4.3).

**Tablo 4.2.** *İç Denetçinin YRU sorumlulukları Anketi KGO ve KGİ*

| Madde No | Uygun Görüşü Bildiren Kişi Sayısı | KGO | Madde No | Uygun Görüşü Bildiren Kişi Sayısı | KGO | Madde No | Uygun Görüşü Bildiren Kişi Sayısı | KGO |
|---|---|---|---|---|---|---|---|---|
| 1 | 19 | 0.90 | 32 | 15 | 0.50 | 63 | 19 | 0.90 |
| 2 | 18 | 0.80 | 33 | 16 | 0.60 | 64 | 16 | 0.60 |
| 3 | 18 | 0.80 | 34 | 15 | 0.50 | 65 | 17 | 0.70 |
| 4 | 18 | 0.80 | 35 | 16 | 0.60 | 66 | 16 | 0.60 |
| 5 | 19 | 0.90 | 36 | 17 | 0.70 | 67 | 12 | 0.20* |
| 6 | 9 | -0.10* | 37 | 12 | 0.20* | 68 | 9 | -0.10* |
| 7 | 16 | 0.60 | 38 | 16 | 0.60 | 69 | 11 | 0.10* |
| 8 | 15 | 0.50 | 39 | 13 | 0.30* | 70 | 18 | 0.80 |
| 9 | 17 | 0.70 | 40 | 13 | 0.30* | 71 | 18 | 0.80 |
| 10 | 18 | 0.80 | 41 | 15 | 0.50 | 72 | 16 | 0.60 |
| 11 | 19 | 0.90 | 42 | 13 | 0.30* | 73 | 14 | 0.40* |
| 12 | 15 | 0.50 | 43 | 11 | 0.10* | 74 | 16 | 0.60 |
| 13 | 15 | 0.50 | 44 | 16 | 0.60 | 75 | 18 | 0.80 |
| 14 | 19 | 0.90 | 45 | 13 | 0.30* | 76 | 16 | 0.60 |
| 15 | 18 | 0.80 | 46 | 18 | 0.80 | 77 | 11 | 0.10* |
| 16 | 20 | 1.00 | 47 | 20 | 1.00 | 78 | 13 | 0.30* |
| 17 | 20 | 1.00 | 48 | 19 | 0.90 | 79 | 11 | 0.10* |
| 18 | 19 | 0.90 | 49 | 14 | 0.40* | 80 | 16 | 0.60 |
| 19 | 15 | 0.50 | 50 | 14 | 0.40* | 81 | 15 | 0.50 |
| 20 | 16 | 0.60 | 51 | 17 | 0.70 | 82 | 14 | 0.40* |
| 21 | 13 | 0.30* | 52 | 16 | 0.60 | 83 | 15 | 0.50 |
| 22 | 12 | 0.20* | 53 | 18 | 0.80 | 84 | 11 | -0.20* |
| 23 | 16 | 0.60 | 54 | 15 | 0.50 | 85 | 14 | 0.80 |
| 24 | 14 | 0.40* | 55 | 16 | 0.60 | 86 | 12 | 0.20* |
| 25 | 13 | 0.30* | 56 | 15 | 0.50 | 87 | 14 | 0.40* |
| 26 | 16 | 0.60 | 57 | 16 | 0.60 | 88 | 11 | 0.10* |
| 27 | 17 | 0.70 | 58 | 17 | 0.70 | 89 | 12 | 0.20* |
| 28 | 15 | 0.50 | 59 | 18 | 0.80 | 90 | 15 | 0.50 |
| 29 | 13 | 0.30* | 60 | 15 | 0.50 | 91 | 12 | 0.20* |
| 30 | 15 | 0.50 | 61 | 19 | 0.90 | | | |
| 31 | 13 | 0.30* | 62 | 20 | 1.00 | | | |
| **Katılımcı Sayısı 20**<br>**Kapsam Geçerlilik Ölçütü 0,42**<br>**Kapsam Geçerlilik İndeksi 0,69** | | | | | | | | |

***** 0,05 düzeyinde anlamlı olmayan maddeler

Uzman görüşlerinden elde edilen verilerin değerlendirilmesi sonucunda madde havuzunda uzlaşı istatistikleri düşük bulunan toplam 38 madde ölçekten çıkarılmıştır. Son olarak uzlaşı istatistikleri kritik değerin üzerinde kalan ancak uzmanlarla yapılan görüşmelerde anlam sorunu oluşturabilecek ve diğer maddelerle birlikte ele alındığı

zaman ölçekte olmasına gerek görülmeyen sorular, madde havuzundan çıkarılmıştır. Böylelikle 45 maddelik iç denetçilerin YRU sorumlulukları ölçeği ve 12 maddelik YRU yaklaşımının faydaları ölçeği elde edilmiştir. Veri toplama aracı, çalışmanın sonunda bulunan EK-1'de sunulmuştur.

**Tablo 4.3.** *YRU Yaklaşımının Faydaları Anketi KGO ve KGİ*

| Madde No | Uygun Görüşü Bildiren Kişi Sayısı | KGO | Madde No | Uygun Görüşü Bildiren Kişi Sayısı | KGO |
|---|---|---|---|---|---|
| 1 | 16 | 0.60 | 13 | 16 | 0.60 |
| 2 | 17 | 0.70 | 14 | 15 | 0.50 |
| 3 | 15 | 0.50 | 15 | 15 | 0.50 |
| 4 | 15 | 0.50 | 16 | 16 | 0.60 |
| 5 | 11 | 0.10* | 17 | 12 | 0.20* |
| 6 | 13 | 0.30* | 18 | 17 | 0.70 |
| 7 | 13 | 0.30* | 19 | 15 | 0.50 |
| 8 | 13 | 0.30* | 20 | 12 | 0.20* |
| 9 | 11 | 0.10* | 21 | 12 | 0.20* |
| 10 | 13 | 0.30* | 22 | 16 | 0.60 |
| 11 | 18 | 0.80 | 23 | 14 | 0.40* |
| 12 | 11 | 0.10* | 24 | 13 | 0.30* |
| **Katılımcı Sayısı 20<br>Kapsam Geçerlilik Ölçütü 0,42<br>Kapsam Geçerlilik İndeksi 0,59** | | | | | |

* 0,05 düzeyinde anlamlı olmayan maddeler

Lawshe tekniğiyle uzman görüşlerinden elde edilen verilerin değerlendirilmesi sonucunda, oluşturulan veri derleme aracının, araştırma örneklemi tarafından çalışmanın amaçlarına uygun şekilde anlaşılıp anlaşılmadığı, uzman görüşü alınmadan önce yapıldığı gibi, az sayıda iç denetçi üzerinde saha çalışması yapılarak tekrar değerlendirilmiştir. Soru ifadelerinin uygunluğunu bir defa daha test etmek amacıyla, yüz yüze görüşme yapılarak, bir yükseköğretim kurumunun iç denetçilerinden ve özel sektörde çalışan TİDE üyesi az sayıda iç denetçiden veri derleme aracını yanıtlamaları istenmiştir. Görüşme sırasında ölçek maddelerinin herhangi bir olumsuz özelliğe sahip olup olmadığı, denetçiler tarafından tek tek değerlendirilmiş ve uygun görülen öneriler tarafımızca dikkate alınmıştır.

### 4.2.3. Araştırmanın Evreni ve Örneklemi

Bilimsel araştırmanın planlanması sürecinde araştırma evreninin belirlenmesi ve evrenden örneklem seçimi önemli bir aşamadır. Evren araştırma kapsamında olan konuyu oluşturan elemanların tümünü kapsayan yapı veya araştırma sonuçlarının genellenmek istendiği elemanların tamamı olarak ifade edilebilir. Araştırmacılar elde ettikleri bulguları geniş bir evrene genellemek isterler. Ancak emek, maliyet ve zaman kısıtları evrenin seçiminde idealist değil rasyonel bir tercih yapılmasını zorunlu kılar. İki tür evrenden söz edilebilir. Bunlardan ilki, tanımlanması kolay ancak ulaşılması çoğu zaman imkânsız olan araştırma evreni ya da genel evrendir. İkincisi ise, araştırma evreninin niteliklerini yansıtan ve ulaşılabilirliği olan çalışma evrenidir. Evrenin özelliklerini taşıyan bir örneklem seçiminin yapılabilmesi ve araştırma bulgularının evrene genellenebilmesi için evrenin sınırlarının mutlaka doğru belirlenmesi gerekir (Özen & Gül, 2007, s. 395).

Çalışmamızın genel evrenini iç denetçiler, bağımsız denetçiler ve işletme yöneticileri oluşturur. Çalışma kapsamında iç denetçilerin sorumluluklarının YRU yaklaşımının faydalarıyla ilişkisi yapısal model aracılığıyla test edildikten sonra, iç denetimin sorumlulukları hakkında olması gereken ve uygulamadaki duruma ilişkin iç denetçilerin görüşlerinin yanında bağımsız denetçiler ve işletme yöneticilerinin görüşlerine başvurulmuştur. Çalışmanın amaçları ve kapsamı dikkate alınarak, iç denetim hizmetlerini alan işletme yöneticilerinin ve mesleki çalışmaları sebebiyle iç denetimi incelemek zorunda olan bağımsız denetçilerin görüşlerine başvurularak, çalışmanın değerini ve nesnelliğini artırmak amaçlanmıştır.

Emek, maliyet ve zaman kısıtları dikkate alınarak araştırmamızın çalışma evreni; TİDE üyesi iç denetçiler, KGK'dan yetki belgesi alan ve fiili olarak bağımsız denetim işiyle uğraşan bağımsız denetçiler ve Borsa İstanbul'da hisseleri işlem gören şirketlerin yöneticileri olarak belirlenmiştir. TİDE'nin 2018 yılı faaliyet raporuna göre, 2667 iç denetçi TİDE'ye üyedir. KGK'nın internet sitesindeki bilgilere göre 16170 bağımsız denetçi yetki belgesine sahiptir, ancak bunların bir kısmının faal olmadığı anlaşıldığından net sayı belirlenememiştir. KAP'taki bilgilere göre 2019 yılı itibariyle Borsa İstanbul'da 399 şirketin hissesi işlem görmektedir, ancak her şirkette kaç üst yönetici olduğu bilinemediğinden yine işletme yöneticilerinin net sayısı belirlenememiştir.

Çalışmamız kapsamında yürütülen istatistiksel analizlerin uygun şekilde yürütülebilmesi için belirli örneklem büyüklüğüne ulaşılması gerekmektedir. Ayrıca örneklem büyüklüğü, araştırma modelinin test edilmesi için yürütülen YEM

kapsamındaki analizlerde tahmin modelinin değişmesine yol açan analiz türü seçimini etkileyen varsayımlardan birisidir. YEM'de normallik ve kayıp verinin miktarı gibi örneklem büyüklüğünün artırılmasını gerektiren varsayımlar sağlansa bile yine de doğru bir biçimde belirlenmiş modeller ve çok değişkenli normal dağılmış veri için yapılan çalışmalar örneklem büyüklüğüyle ilgili sınırlamalar getirmiştir. Yapılan çalışmalar, makul örneklem büyüklüğünün 150 (Muthen & Muthen, 2002) veya 200 (Hoogland & Boomsma, 1998) olması gerektiğini öne sürmüştür. Yine litaratürde yer alan bazı çalışmalar, YEM uygulamaları için 100'ün altındaki örneklemleri küçük, 100-200 arasını orta ve 200'den fazla örneklemleri büyük olarak nitelendirmiştir (Aksu, Eser & Güzeller, 2017, s. 70). Araştırmanın veri toplama formu makul araştırma süresi içerisinde mümkün olduğunca çok katılımcıya doldurtularak, yürütülen tüm betimsel ve yordayıcı istatistiksel analizlerin yapılabileceği yeterli örneklem sayısına ulaşılmıştır.

İç denetçilerden veri toplamak amacıyla TİDE'den yardım alınmıştır. TİDE elektronik ortama taşıdığımız veri toplama formunu, üyelerine 2 kez göndermiş ve daha fazla katılımcıya ulaşmamız için bazı üyelerinden özellikle ricada bulunmuştur. Bunun dışında Türkiye İç Denetim Kongresinde ve iç denetçilerin katılacağı bazı toplantılarda yüz yüze görüşme yoluyla katılımcı sayısı artırılmıştır. İç denetçilerden veri toplanırken çalışma evreninin tamamına ulaşılarak, araştırmaya katılmaya istekli olan iç denetçiler ile iletişime geçilmiştir. Hatalı ve eksik doldurulan formlar çıkarıldıktan sonra toplamda 247 iç denetçiden veri elde edilmiştir.

Bağımsız denetçilerin iletişim bilgilerine YMM Odaları ve dört büyük denetim firmasının Türkiye şubelerinden ulaşılmıştır. İşletme yöneticilerinin iletişim adreslerine ise KAP'ın yayınladığı şirketlerin bağlantı kurulacak yetkili bilgilerinden ve şirketlerin kendi internet sitelerinden ulaşılmıştır. Daha önce ifade ettiğimiz üzere, bağımsız denetçiler ve işletme yöneticileri için evrenin tam bir listesi oluşturulamadığından olasılıklı örnekleme yöntemlerine başvurulamamıştır. Örneklem seçiminde kartopu örnekleme yöntemi kullanılmıştır. Veri toplama formları katılımcılara yüz yüze ve e-posta ile ulaştırılmıştır. Katılımcılara telefonla ulaşılmış, çalışma hakkında bilgi verilmiş ve yanıt vermeleri istenmiştir. Veri toplama süreci sonunda hatalı ve eksik formlar çıkarıldıktan sonra toplamda 72 işletme yöneticisinden ve 96 bağımsız denetçiden veri elde edilmiştir. Araştırma örnekleminin demografik özellikleri Tablo 4.4'te yer almaktadır.

**Tablo 4.4.** *Araştırma Örnekleminin Demografik Özellikleri*

| | İç Denetçi (n=247, %59) | Bağımsız Denetçi (n=96, %23) | İşletme Yöneticisi (n=72, %18) |
|---|---|---|---|
| **Cinsiyet** | | | |
| Kadın | 84, %34 | 30, %31 | 20, %28 |
| Erkek | 163, %66 | 66, %69 | 52, %72 |
| **Yaş** | | | |
| 30 altı | 36, %14 | 3, %3 | 0, |
| 31-35 arası | 56, %23 | 7, %7 | 3, %4 |
| 36-40 arası | 68, %28 | 17, %18 | 7, %10 |
| 41-45 arası | 38, %15 | 23, %24 | 17, %24 |
| 46-50 arası | 22, %9 | 16, %17 | 14, %20 |
| 51-55 arası | 22, %9 | 15, %15 | 11, %15 |
| 56 üstü | 5, %2 | 15, %15 | 20, %28 |
| **Mesleki Deneyim** | | | |
| 5 altı | 41, %17 | 3, %3 | 0 |
| 6-10 arası | 81, %33 | 15, %16 | 4, %5 |
| 11-15 arası | 49, %20 | 10, %11 | 5, %7 |
| 16-20 arası | 17, %7 | 24, %25 | 23, %32 |
| 21-25 arası | 15, %6 | 17, %18 | 12, %17 |
| 26 üstü | 10, %4 | 27, %28 | 28, %39 |
| Cevaplamayan | 34, %14 | 0 | 0 |
| **Toplam** | **247, %59** | **96, %23** | **72, %18** |

### 4.2.4. Veri Analizi

İç denetçilerin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini ortaya çıkarmayı amaçlayan ilgili kuramı YEM ile test etmek amacıyla öncelikle veri derleme aracında aralarında yüksek korelasyon gösteren yapıları keşfetmek ve faktör puanlarının geçerliliğini değerlendirmek için AFA uygulanmıştır. Ayrıca çalışma kapsamında yapılması tasarlanan, katılımcı gruplarının olması gereken duruma veya uygulamaya yönelik görüşlerinin kıyaslanabilmesini sağlayan bağımsız örneklemler ve eşleştirilmiş örneklemler t testlerinin uygulanabilmesi amacıyla öncelikle AFA ile karşılaştırılacak yapıların ortaya çıkarılması gereklidir.

AFA, belirli bir hipotezi sınamak yerine yapının içinde yer alan faktörlerin doğası ve sayısı hakkında bilgi edinmek için uygulanır. Çalışmamızda AFA, iç denetimin YRU yaklaşımı kapsamında tanımladığımız sorumluluklarına ve YRU yaklaşımının faydalarına ilişkin faktörlerin ortaya çıkarılması için kullanılmıştır.

AFA'dan sonra DFA ve YEM uygulanacağı için, faktör belirleme yordamı olarak Maksimum Olabilirlik (Maximum Likelihood-ML) tercih edilmiştir. ML, normal dağılım gösteren değişkenler üzerinde kullanılması tercih edilen yordamlardan biridir. Veri setinin normal dağılım gösterdiğinin kabul edilmiş olması, ML'nin tercih edilmesi için gereken normallik sayıltısının varsayıldığını gösterir. AFA'da faktörlerin daha kolay

yorumlanması için faktör döndürme yapılmıştır. Faktör döndürme, faktör yapısını değiştirmeden yorumlanmasını kolaylaştırır. Dik Döndürme yöntemleri veriler arasında ilişki olmadığında kullanılır. AFA uygulanırken yorumlanması eğik döndürme yöntemlerine göre daha kolay olan dik döndürme yöntemlerinden birisi olan varimax yöntemi kullanılmıştır.

AFA'dan sonra ölçüm modelinin doğrulanması için DFA uygulanmıştır. DFA, genellikle ölçek geliştirme ve geçerlilik çalışmalarında önceden belirlenmiş veya kurgulanmış bir yapının doğrulanması amacıyla kullanılır. DFA, temelde YEM ile aynı mantığa ve hesaplama tekniğine dayanır. DFA, YEM'in özel bir uygulama alanıdır ve ölçüm modeli de tipik bir DFA olarak ele alınmaktadır. DFA, verinin faktör yapısının hipotez edilen modele uyumunu test etmekte veya doğrulamaktadır (Bayram, 2010, s. 42). DFA'da AFA'dan farklı olarak; (1) gözlenen değişkenler sadece önceden belirlenen gizil değişkenlerle bağlanır, (2) bazı hata terimleri arasında korelasyona izin verilebilir (Blunch, 2012).

YEM, ölçüm modeli ve yapısal model olmak üzere iki bölümden oluşur. Ölçüm modeli, DFA ile test edilir veya doğrulanır. Ölçüm modeli, faktör analizinde faktör olarak isimlendirilen gizil değişkenlerin veya varsayımsal yapıların bir ölçme aracı ifadesi gibi gözlenen değişkenler tarafından nasıl tanımlandığını ve gözlenen değişkenlerin geçerlilik ve güvenilirlik gibi ölçüm özelliklerini tanımlar (Jöreskog & Sörbom, 1996). YEM çözümlemesinin başlangıç noktası olan ölçüm modeli, gizil değişkenlerin arasındaki korelasyon ilişkilerinin hesaplanmasıdır. Yapısal modelde değişkenler arası ilişkilerin test edilmesinden önce, ölçme modelleri test edilmelidir. Yani önce elde edilen verinin değişkenleri doğrulayıp doğrulamadığı ölçüm modelleriyle test edildikten sonra, gizil değişkenler arasındaki teorik olarak tahmin edilen ilişkilerin varlığı yapısal modelde test edilir (Şimşek, 2007, s.12). Çalışmamız kapsamında AFA ile keşfedilen faktörler, DFA ile doğrulanmıştır. Başka bir ifadeyle, DFA ile oluşturulan ölçüm modelleriyle, ölçme araçlarıyla toplanan verinin AFA ile belirlenen gizil değişkenleri doğrulayıp doğrulamadığı ve aralarındaki korelasyonel ilişkiler değerlendirilmiştir.

Ölçüm modelinde yapı geçerliliğinin sağlandığının doğrulanması için 3 ölçüt dikkate alınır. Öncelikle her bir faktör altında yer alan gözlenen değişkenin standartlaştırılmış faktör yükü 0,50'den büyük ve istatistiksel olarak anlamlı olmalıdır. Her bir gizil değişkenin yapı güvenilirliğinin değerlendirilmesi gereklidir. DFA'da faktörlerin yapı güvenilirliği birleşik güvenilirlik (composite reliability) değerine göre

değerlendirilmiştir. Güvenilir faktörlerin birleşik güvenilirlik değerlerinin 0,70'de büyük olması beklenir. Son olarak, her bir gizil değişkenin açıkladığı varyansın (AVE- Average Variances Explanied) 0,50'dan fazla olması gerekmektedir (Fornell & Larcher, 1981; Hair vd, 2013).

Birleşik güvenilirlik değeri, gizil değişkenler içerisinde gözlenen değişkenlerin temsil ettiği önermelerin kendi içerisinde iç tutarlılığını, geçerliliğini ve güvenilirliğini ölçmektedir. Birleşik güvenilirlik değeri; sayıca birden fazla, heterojen, ancak benzer önermelerin güvenilirliğinin ölçülmesinde, Alpha değerine bir alternatif ya da kontrol aracı olarak kullanılmaktadır. Birleşik güvenilirlik, Fornell & Larcher'in formülüyle (1981, s. 40) kolayca hesaplanabilir:

$$CR = \frac{(\sum \text{ Standardize yük Değerleri })^2}{(\sum \text{ S.Yük D.})^2 + (\sum \text{Hata Varyansları})}$$

Standardize edilmiş faktör yükleri, t-istatistikleri, açıklanan varyans ve birleşik güvenilirlik değerleri ölçüm modeli veya yapısal modelin kabul edilmesi için yeterli değildir. Modelin veri ile uyumu, uyum iyiliği istatistikleriyle doğrulanmalıdır. Uyum iyiliği değerleri, bir modelin bir bütün olarak araştırma verisi tarafından uygun seviyede onaylandığı konusunda değerlendirmeler yapılmasını sağlar (Hu & Bentler, 1999). Çalışmamızın ölçüm modelleri ve yapısal modeli, uyum iyiliği istatistikleriyle değerlendirilmiştir. Araştırma modelimizi doğrulamak için kullandığımız uyum iyiliği istatistikleri ve kabul edilebilir sınırlar Tablo 4.5'te sunulmuştur (Byrne, 2011; Çelik & Yılmaz, 2013; Jöreskog & Sörbom, 1996; Hair vd., 2013; Raykov & Marcoulides, 2006). Ayrıca çalışmamızda olduğu gibi, 30 veya daha fazla gözlenen değişkene sahip modeller için daha düşük uyum sınırlarının kabul edilebileceği savunulmaktadır (Yaşlıoğlu, 2017).

**Tablo 4.5.** *Uyum İyiliği Değerleri*

| Uyum İndeksleri | İyi Uyum | Kabul Edilebilir Uyum |
|---|---|---|
| **χ 2/sd** | 0<χ 2/sd<2 | 0<χ 2/sd<3 |
| **CFI** | 0.97<CFI<1 | 0.95<CFI<1 |
| **GFI** | 0.95<GFI<1 | 0.90<GFI<1 |
| **NFI** | 0.95<NFI<1 | 0.90<NFI<1 |
| **NNFI** | 0.97<NNFI<1 | 0.95<NNFI<1 |
| **RMSEA** | 0<RMSEA<0.05 | 0<RMSEA<0.08 |
| **RMR** | 0<RMR<0.05 | 0<RMR<0.05 |
| **SRMR** | 0<SRMR<0.05 | 0<SRMR<0.05 |

$\chi 2$ en yaygın kullanılan ve bir anlamda başlangıç uyum indeksi sayılabilecek bir istatistiktir (Meydan & Şeşen, 2015, s. 32). Ancak $\chi 2$'nin bazı sınırlılıkları vardır. Özellikle örneklem ile modele ilişkin kovaryans matrisi arasındaki uyumsuzluğun önemsiz olduğu hallerde $\chi 2$, makul bir modelin reddedilmesine neden olabilir. Jöreskog & Sörbom (1996), $\chi 2$'nin biçimsel bir test gibi kullanılamayacağını örnekleme dağılımının beklenen değeriyle karşılaştırılması gerektiğini savunmuştur. Bunun için $\chi 2$/sd kullanılabilir (Bagozzi, 1981, s. 380).

İstatistik literatüründe farklı sınırlamaları gidermeyi amaçlayan alternatif uyum iyiliği istatistikleri geliştirilmiştir. Uyum iyiliği istatistiklerinin birbirlerine karşı üstünlükleri vardır ve bu yüzden birlikte değerlendirilirler. Ölçüm modellerimizin ve yapısal modelimizin veri ile genel uyumunu değerlendirmek için kullandığımız RMSEA (Yaklaşık Hataların Ortalama Karekökü/Root Mean Square Error of Approximation), RMR (Ortalama Hataların Karekökü/Root Mean Square Residual), SRMR (Standardize Edilmiş Ortalama Hataların Karekökü/Standardized Root Mean Square Residual), GFI (İyilik Uyum İndeksi/Goodness of Fit Index), CFI (Karşılaştırmalı Uyum İndeksi/ Comparative Fit Index), NFI (Normlaştırılmış Uyum İndeksi/Normed Fit Index) ve NNFI (Normlaştırılmamış Uyum İndeksi/Non-Normed Fit Index) değerleri literatürde en fazla kullanılan uyum iyiliği istatistiklerindendir (Jöreskog & Sörbom, 1996; Hair vd., 2013; Raykov & Marcoulides, 2006).

RMSEA, evrendeki yaklaşık uyumun bir ölçümüdür; RMR, gözlenen kovaryans ile tahmin edilen kovaryans arasındaki farktır; SRMR ise, RMR değerinin standardize edilmiş halidir. GFI, modelin açıkladığı varyans ve kovaryans büyüklüğünün bir göstergesidir, regresyondaki $R^2$ ile benzerdir. NFI, doymuş model ile bağımsız model arasındaki mevcut modelin göreli konumunu gösterir; NNFI, NFI'nın sınırlılıklarına karşı modele serbestlik derecesini ilave eder; CFI ise, NFI ve NNFI ile benzer ama çok daha katı bir istatistiktir (Bayram, 2010, s. 76).

Çalışmanın yapısal modeli test edildikten sonra, örneklem gruplarının ve aynı grubun farklı durumlara ilişkin görüşleri AFA ile elde edilen faktör yapıları üzerinden t testleri aracılığıyla test edilmiştir. İç denetçilerden oluşan ile bağımsız denetçiler ve işletme yöneticilerinden oluşan grupların görüşlerini veya aynı grubun olması gereken duruma ve sahadaki duruma ilişkin görüşlerini karşılaştırmak amacıyla uyguladığımız t testlerinin sonuçlarıyla yetinilmemelidir. Veri derleme aracıyla elde edilen görüşlerin

ortalamaları arasında istatistiksel olarak anlamlı bir ilişkinin varlığı, her zaman kuram ve uygulamada önemli olduğu anlamına gelmeyebilir (Huck, 2008).

Ortalamalar arasında istatistiksel olarak anlamlı farkın etki büyüklüğünün ölçülmesi gerekir. Etki büyüklüğü, bağımsız değişkenin bağımlı değişkende neden olduğu anlamlı değişimin veya iki veri grubu arasındaki anlamlı farkın büyüklüğünü belirlemeye yarar. En yaygın kullanılan etki büyüklüğü istatistiklerinden biri, çalışmamızda kullandığımız Cohen d'dir. Cohen d değerinin yorumlanmasında kullanılan rehber değerlere göre, 0,2=küçük; 0,5=orta ve 0,8=büyük etkiye işaret eder (Cohen, 1988).

## 5. BULGULAR

YEM, değişkenler arasında teorik olarak var olması beklenen ilişki örüntüsünü tanımlayan modellerin doğrulanmasında yararlanılan çok değişkenli istatistiksel bir tekniktir. YEM, ölçme ve yapısal model olmak üzere iki alt modelden oluşur. Ölçüm modeli, DFA'nın en yalın halidir. Yapısal model ise, örtük değişkenler arası ilişkilerin test edildiği aşamadır. YEM, açıklayıcı olmaktan çok doğrulayıcı bir tekniktir. YEM araştırmacılar tarafından daha çok uygun bir model bulmak yerine, teorik olarak ortaya konan modellerin araştırma verileriyle uyumu yani modelin doğrulanması için tercih edilmektedir. Teoride yer alan bir modelin doğrulanması yerine model keşfetmeyi amaçlayan bir çalışmada, öncelikle araştırma verileri içerisinde yer alan yapıların keşfedilmesi için AFA yürütülmelidir.

Bu bölümde elde edilen veri setinin içerisinde yer alan yapıları ortaya çıkarmak amacıyla yürütülen AFA; gözlenen değişkenler ile gizil değişkenler arasında ilişki örüntüsünü değerlendirmek amacıyla yürütülen DFA ve öngörülen modelde yer alan hipotetik ilişkileri test etmek amacıyla yürütülen YEM'den elde edilen araştırma bulgularına yer verilmiştir. İç denetçilerin yönetişim, risk yönetimi, uygunluk ve teknolojiye ilişkin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisi, tasarlanan bir araştırma modeliyle iç denetçilerden oluşan araştırma örneklemi üzerinde test edilmiş ve bulguları yorumlanmıştır. Ayrıca örneklem gruplarının görüşlerinin ortalamaları ve olması gereken durum ile uygulamadaki duruma yönelik görüşlerin ortalamaları arasındaki farklılığın anlamlı olup olmadığını test etmek amacıyla yürütülen t testlerinin bulguları raporlanmıştır. İç denetçilerin olması gereken duruma ilişkin görüşleri, hem uygulamadaki duruma ilişkin görüşleriyle hem de işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun görüşleriyle karşılaştırılmıştır. Araştırma bulguları elden geldiğince açık, anlaşılır ve ihtiyaca göre tablolar ve şekiller kullanılarak sunulmuştur.

### 5.1. Veri Dağılımı, Geçerlilik ve Güvenilirlik

Veri derleme aracıyla toplanan verilerle istatistiksel analizler uygulanmadan önce, hem faktör analizi hem de bağımsız örneklemler ve eşleştirilmiş örneklemler t testleri için önkoşul olan sayıltıların başında gelen normallik test edilmiştir. Araştırmanın likert tipi ölçekle kurgulanması sonucunda araştırma verileri, değerlerin önem derecesi ya da üstünlüklerini baz alan sıralı (ordinal) değişkenlerden oluşmuştur. Bu nedenle verilerin dağılımı, normalliği ölçen test istatistikleri yerine grafiksel yaklaşımla ve basıklık-çarpıklık değerleriyle incelenmiştir.

Tabachnik & Fidell (2013, s. 81), araştırma verilerinin dağılımının grafikler incelenerek değerlendirilmesi gerektiğini önerir. Bu amaçla ölçme aracında yer alan her bir ifadeye ilişkin toplanan verinin dağılımı, histogram ve Q-Q plot grafikleri incelenerek değerlendirilmiştir. Grafikler incelendiğinde verilerin normal dağılıma yakın bir dağılım gösterdiği ve normallik sayıltısının ihlal edilmediği sonucuna ulaşılmıştır.

Çarpıklık (skewness) ve basıklık (kurtosis) değerleri de normal dağılım hakkında bilgi verir. Çarpıklık dağılımın simetrisi, basıklık ise sivriliğini ölçer. Verilerin dağılımı mükemmel seviyede normal dağılım gösteriyorsa, bu değerler 0 olarak hesaplanır, ancak özellikle sosyal bilimlerde bu durum neredeyse imkânsızdır. İstatistik literatüründe yapılan birçok çalışmada çarpıklık ve basıklık sınır değerleri, yapılan analizler sonucunda elde edilen deneyimlere göre yeniden değerlendirilmiştir. Literatürde, sınır değerlerin +1 ile -1 arasında (Hair vd., 2013), +1,5 ile -1,5 arasında (Tabachnik & Fidell, 2013), +2 ile -2 arasında (George & Mallery, 2010) olması gerektiğini savunan çalışmalar vardır. Çalışmamız kapsamında toplanan verilerin çarpıklık ve basıklık değerleri incelendiğinde, verilerin büyük çoğunluğunun +1 ile -1 arasında olduğu, bazılarının +1,5 ile -1,5 arasında olduğu ve çok az bir kısmının (yaklaşık %3) +2 ile -2 arasında olduğu belirlenmiş ve normallik sayıltısının ihlal edilmediği varsayılmıştır.

Ayrıca YEM analizlerinin önemli bir varsayımı çok değişkenli normalliktir. Sosyal bilimlerde sıklıkla kullanılan sıralı değişkenlerin varlığı çoklu normallik varsayımını tehdit eder. Varsayımın ihlali modelin değerlendirilmesinde kullanılan bazı uyum indekslerini olumsuz etkiler. YEM analizleri öncesinde veri setinde yer alan değişkenlerin, çok değişkenli normalliği test edilmiş ve varsayımın ihlal edilmediği sonucuna varılarak analizlere geçilmiştir.

YEM analizleri ile AFA ve DFA sonuçlarını etkileyen önemli bir konu, veri setinde bulunan kayıp verilerin değerlendirilmesidir. Veri toplama sürecinde, katılımcılar

tarafından özenli şekilde yanıtlanmayan büyük oranda eksik doldurulan formlar, değerlendirmeye alınmamıştır. Veri seti üzerinde yapılan kayıp veri analizleri sonucunda kayıp değerlerin %1'den az olduğu tespit edilmiştir. YEM analizlerinin kayıp veriye yüksek hassasiyet göstermesi nedeniyle, kayıp veri ataması yapılmıştır. Kayıp veri atamasında eksik yanıtlar yerine, değişkenin mod değeri atanmıştır. En fazla verilen yanıtın, örneklemin görüşünü daha fazla temsil edeceği varsayılmıştır.

Veri derleme aracının yapı geçerliliğini ölçmek ve boyutlarını belirlemek için AFA kullanılmıştır. Veri derleme aracının, dayandığı kuramsal çerçeveyi ölçebilmesi geçerli olduğu anlamına gelir. Geçerlilik analizi, araştırmada kullanılan veri derleme aracının ölçülmesi amaçlanan görüşleri başka şeylerle karıştırmadan ölçebilme düzeyinin tespit edilmesidir. Faktör analizinin arkasında yer alan görüş, ölçülebilir ve gözlemlenebilir değişkenlerin gözlemlenebilir olmayan daha az sayıda gizil değişkenle ifade edilebileceğidir. Yani boyutsallığın indirgenmesi olarak tanımlanan bu görüşe göre, çok sayıda gözlenen değişken az sayıda gizil değişkene indirgenebilir. Faktör analizi, birbiriyle ilişkili çok sayıda değişkeni tek bir genel değişken ya da kavram altında toplar. Amacı, tüm değişkenlerin yer aldığı uzayın kaç boyutlu bir yapıya sahip olduğunu ortaya çıkararak yeni uzay hakkında yorum yapılabilmesini sağlamaktır (Aksu, Eser & Güzeller, 2017, s. 2).

Veri derleme aracının güvenilirliğinin önemli bir göstergesi iç tutarlılıktır. İç tutarlılık, veri derleme aracında bulunan her ifadenin her ölçümde, aynı amaçlanan özelliği ölçebilme derecesidir. Çok çeşitli yollarla ölçülebilen iç tutarlılık için en fazla kullanılan yöntemlerden biri Cronbach Alpha katsayısıdır. Alpha katsayısı, ölçme aracında yer alan tüm ifadeler arasındaki ortalama korelasyonun göstergesidir. Ölçme araçları, amaçları gereği farklı seviyede güvenilirlik katsayısı gerektirse de, madde sayısına bağlı olarak Alpha'nın 0,70'in üzerinde olması önerilir (Pallant, 2016, s. 18). Araştırmamız kapsamında veri derleme aracımızı oluşturan iki ölçek için Alpha değerleri hesaplanmıştır. Alpha katsayısı, İç Denetimin Sorumlulukları Ölçeği için 0,861, YRU Yaklaşımının Faydaları Ölçeği için 0,945 olarak hesaplanmıştır. Ayrıca ölçekleri oluşturan her bir faktör için hesaplanan Alpha katsayılarını yüksek güvenilirlik düzeyine ulaşıldığını gösterir. Ayrıca ölçüm modelinde yer alan her bir faktör için Alpha değerine bir alternatif ya da kontrol aracı olarak kullanılan birleşik güvenilirlik değerleri hesaplanmış ve yüksek güvenilirlik düzeyi doğrulanmıştır.

### 5.2. İç Denetimin Sorumluluklarına İlişkin Açımlayıcı Faktör Analizi

Ölçme aracının faktör yapılarını ortaya çıkarmak ve yapı geçerliliğini ölçmek amacıyla AFA yapılmadan önce, verinin faktör analizine uygunluğunu değerlendiren Kaiser-Meyer-Olkin (KMO) ve Bartlett testlerinden elde edilen sonuçlar yorumlanmıştır. KMO testi, örneklemin faktör analizi için yeterliliğini sınar. KMO değerinin 0,6'dan büyük olması gerekir ve 1'e ne kadar yaklaşırsa örneklemin faktör analizi için yeterliliğinin o kadar yüksek olduğu yorumu yapılır. KMO değerinin 0,5-0,7 arası olması normal, 0,7-0,8 arası iyi, 0,8-0,9 arası çok iyi ve 0,9'dan büyük olması mükemmel olarak yorumlanır (Hutcheson & Sofroniou, 1999). İç Denetimin Sorumlulukları ölçeğinin KMO değeri 0,859 olarak hesaplanmıştır. Küresellik sınaması olarak bilinen Bartlett Testi, değişkenlerin birbiriyle ilişkili olup olmadığını yani faktörler altında ifade edilip edilemeyeceğini gösterir. Bartlett Değeri 5139; $p<0.001$ olarak hesaplanmıştır. Her iki değer, verinin faktör analizine uygunluğunu gösterir.

En uygun faktör yapısına ulaşmak amacıyla faktör yükleri 0,50'den düşük olan maddeler ölçekten çıkarılmıştır. Birden fazla faktör altında yüksek yüklere sahip olan ve yükleri arasında 0,10'un altında fark olan binişik maddeler ölçekten atılmıştır. Ayrıca başka bir faktör belirleme ölçütü olan Kaiser dikkate alınarak yalnızca öz değeri birin üzerinde olan faktörler tutulmuştur.

**Tablo 5.1.** *İç Denetimin Sorumluluklarının Açımlayıcı Faktör Analizi Sonuçları*

| Ölçek Maddeleri | US | BTS | PRS | YS | NRS |
|---|---|---|---|---|---|
| **U8** | ,821 | | | | |
| **U5** | ,785 | | | | |
| **U3** | ,784 | | | | |
| **U12** | ,780 | | | | |
| **U10** | ,767 | | | | |
| **U7** | ,757 | | | | |
| **U9** | ,740 | | | | |
| **BT6** | | ,839 | | | |
| **BT9** | | ,826 | | | |
| **BT3** | | ,797 | | | |
| **BT5** | | ,794 | | | |
| **BT7** | | ,770 | | | |
| **BT1** | | ,704 | | | |
| **BT2** | | ,690 | | | |
| **R1** | | | ,806 | | |
| **R3** | | | ,769 | | |
| **R11** | | | ,768 | | |
| **R4** | | | ,721 | | |
| **R2** | | | ,716 | | |
| **R6** | | | ,699 | | |
| **Y9** | | | | ,829 | |
| **Y7** | | | | ,797 | |
| **Y6** | | | | ,763 | |
| **Y3** | | | | ,758 | |
| **Y4** | | | | ,718 | |
| **Y8** | | | | ,717 | |
| **R9** | | | | | ,826 |
| **R7** | | | | | ,766 |
| **R8** | | | | | ,763 |
| **R10** | | | | | ,759 |
| **R13** | | | | | ,704 |
| **Açıklanan Varyans (%)** | 14,392 | 14,240 | 11,768 | 11,756 | 9,773 |
| **Açıklanan Toplam Varyans (%)** | 61,929 | | | | |
| **Kaiser-Meyer-Olkin (KMO) Test** | 0,859 | | | | |
| **Barlett's Test of Sphericity** | $\chi$ 2 (465)= 5139; (P<0.001) | | | | |
| **Cronbach's Alpha** | 0,919 | 0,919 | 0,897 | 0,895 | 0,880 |

Tablo 5.1'de özetlendiği üzere, iç denetçilerin sorumlulukları, AFA sonucunda toplam varyansın 61,93'ünü açıklayan 5 faktör altında yer alan 31 maddeyle ifade edilmektedir. Faktörleri oluşturan değişkenler incelendiğinde, bunların çalışmamızın kurgusuna uygun şekilde iç denetçilerin sorumluluklarını ifade eden önermeler olduğu anlaşılmaktadır. Bu aşamada ilgili literatür ve uzman görüşleri doğrultusunda faktörler isimlendirilmiştir. Birinci faktörde kümelenen değişkenlerin iç denetimin uygunluğa ilişkin sorumlulukları, ikinci faktörde kümelenen değişkenlerin bilgi teknolojilerine ilişkin sorumlulukları, üçüncü faktörde kümelenen değişkenlerin risk yönetimine ilişkin sorumlulukları, dördüncü faktörde kümelenen değişkenlerin yönetişime ilişkin sorumlulukları ve beşinci faktörde kümelenen değişkenlerin iç denetimin risk

yönetiminde üstlenmemesi gereken sorumluluklar olduğu anlaşılır. Bu nedenle bu faktörler sırasıyla; 'Uygunluk Sorumlulukları', 'Bilgi Teknolojileri Sorumlulukları', 'Risk Yönetimi Sorumlulukları', 'Yönetişim Sorumlulukları' ve 'Üstlenilmemesi Gereken Risk Yönetimi Sorumlulukları' olarak isimlendirilmiştir.

### 5.3. YRU Yaklaşımının Faydalarına İlişkin Açımlayıcı Faktör Analizi

YRU Yaklaşımının Faydaları ölçme aracının faktör yapılarını ortaya çıkarmak ve yapı geçerliliğini ölçmek amacıyla AFA uygulanmıştır. AFA yapılmadan önce, verinin faktör analizine uygunluğunu değerlendiren Kaiser-Meyer-Olkin (KMO) ve Bartlett testlerinden elde edilen sonuçlar değerlendirilmiştir. KMO Değeri 0,935; Bartlett Değeri 1708; $p<0.001$ olarak hesaplanmıştır. Hesaplanan değerler, verinin faktör analizine uygun olduğunu gösterir. En uygun faktör yapısına ulaşmak için faktör belirleme kriterleri dikkate alınmıştır. Buna göre; (1) yalnızca öz değeri birin üzerinde olan faktörler tutulmuş, (2) faktör yükleri 0,50'den düşük olan maddeler ölçekten çıkarılmış ve (3) birden fazla faktör altında yüksek yüklere sahip olan ve yükleri arasında 0,10'un altında fark olan binişik maddeler ölçme aracından çıkarılmıştır.

**Tablo 5.2.** *YRU Yaklaşımının Faydalarının Açımlayıcı Faktör Analizi Sonuçları*

| **Ölçek Maddeleri** | **YRU** |
|---|---|
| YRU12 | ,891 |
| YRU11 | ,890 |
| YRU10 | ,863 |
| YRU7 | ,848 |
| YRU9 | ,840 |
| YRU1 | ,772 |
| YRU6 | ,767 |
| YRU8 | ,756 |
| **Açıklanan Toplam Varyans (%)** | 68,924 |
| **Kaiser-Meyer-Olkin (KMO) Test** | 0,935 |
| **Barlett's Test of Sphericity** | $\chi$ 2 (28)= 1708; (P<0.001) |
| **Cronbach's Alpha** | 0,945 |

Tablo 5.2'te özetlendiği üzere, YRU yaklaşımının faydaları, AFA sonucunda toplam varyansın 68,92'sini açıklayan tek faktör yapısı altında yer alan 8 maddeyle ifade edilmektedir. Ölçme aracında yer alan değişkenler incelendiğinde, bunların YRU Yaklaşımının faydalarını ifade eden önermeler olduğu anlaşılır. Çalışmamızın kurgusuyla tutarlı bir şekilde, elde edilen faktör 'YRU Yaklaşımının Faydaları' olarak isimlendirilmiştir.

Araştırma modelinde yer alan her bir faktöre ilişkin betimleyici istatistikler, Tablo 5.3'te sunulmuştur. Tabloda her bir faktörün ve altında kümelenen maddelerin ortalama ve standart sapma değerleri yer almaktadır. Çalışma Likert tipi ölçekle kurgulandığı için maddelere verilen yanıtlar en düşük bir ve en yüksek beş değerleri arasında yer almaktadır.

**Tablo 5.3.** *Araştırma Modelinde Yer Alan Faktörlerin Betimleyici İstatistikleri*

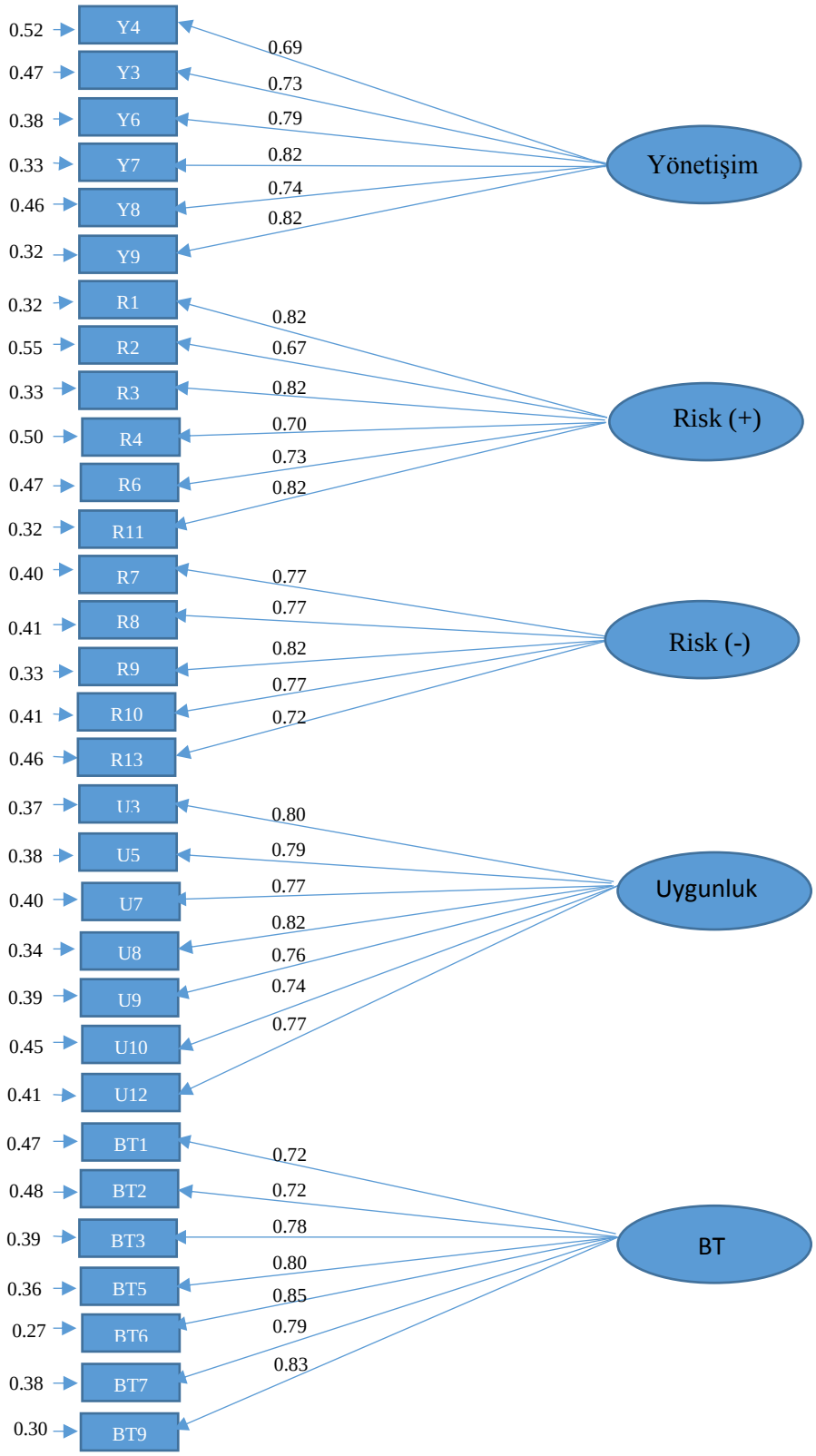
| Faktörler | Ortalama | Standart Sapma | Faktörler | Ortalama | Standart Sapma |
|---|---|---|---|---|---|
| **US** | **4,01** | **0,627** | **YS** | **4,13** | **0,474** |
| U8 | 4,27 | 0,666 | Y9 | 4,53 | 0,539 |
| U5 | 3,64 | 0,867 | Y7 | 3,77 | 0,646 |
| U3 | 4,33 | 0,688 | Y6 | 3,72 | 0,619 |
| U12 | 4,32 | 0,692 | Y3 | 4,48 | 0,540 |
| U10 | 4,26 | 0,702 | Y4 | 4,45 | 0,545 |
| U7 | 3,52 | 0,896 | Y8 | 3,85 | 0,612 |
| U9 | 3,70 | 0,806 | **NRS** | **2,15** | **0,720** |
| **BTS** | **4,45** | **0,511** | R9 | 2,21 | 0,903 |
| BT6 | 4,42 | 0,625 | R7 | 2,17 | 0,868 |
| BT9 | 4,48 | 0,611 | R8 | 2,37 | 0,845 |
| BT3 | 4,41 | 0,598 | R10 | 2,11 | 0,888 |
| BT5 | 4,43 | 0,639 | R13 | 1,88 | 0,873 |
| BT7 | 4,43 | 0,633 | **YRU** | **4,37** | **0,601** |
| BT1 | 4,53 | 0,623 | YRU12 | 4,25 | 0,794 |
| BT2 | 4,46 | 0,629 | YRU11 | 4,41 | 0,674 |
| **PRS** | **4,33** | **0,498** | YRU10 | 4,32 | 0,737 |
| R1 | 4,37 | 0,617 | YRU7 | 4,42 | 0,657 |
| R3 | 4,36 | 0,582 | YRU9 | 4,22 | 0,806 |
| R11 | 4,38 | 0,599 | YRU1 | 4,44 | 0,713 |
| R4 | 4,25 | 0,664 | YRU6 | 4,41 | 0,649 |
| R2 | 4,28 | 0,617 | YRU8 | 4,49 | 0,604 |
| R6 | 4,33 | 0,594 | | | |

Tablo 5.3'te görüldüğü üzere, iç denetimin yönetişim, risk yönetimi, uygunluk ve bilgi teknolojileri sorumluluklarına ilişkin görüşlerin ortalama değerlerinin 4'ün üzerinde olduğu tespit edilmiştir. Likert tipi ölçekte 4'ün 'Katılıyorum'u ifade ettiği düşünüldüğünde, iç denetçilerin görüşlerinin, tanımlanan dört sorumluluk yapısının üstlenilmesi gerektiğini doğrular nitelikte olduğu anlaşılmaktadır. Ayrıca iç denetimin bilgi teknolojileri sorumluluklarını temsil eden BTS faktörünün en yüksek ortalama değerine ($\bar{X}$=4,45) sahip olduğu belirlenmiştir. Diğer taraftan iç denetimin üstlenilmemesi gereken risk yönetimi sorumluluklarını ifade eden NRS faktörüne ilişkin ortalama değerin ($\bar{X}$=2,15) Likert tipi ölçek kurgusunda 'Katılmıyorum'u temsil eden 2 değerine yakınlığı, iç denetçilerin görüşleri ile NRS faktöründe kümelenen sorumlulukların üstlenilmemesi gerektiğini doğruladığını belirtir. Likert tipi ölçek

kurgusunda 4'ün 'Katılıyorum'u ve 5'in 'Kesinlikle Katılıyorum'u temsil ettiği düşünüldüğünde, YRU yaklaşımının faydalarını ifade eden YRU faktörüne ilişkin iç denetçilerin görüşlerinin ortalamalarının ($\bar{X}$=4,37) genellikle olumlu yönde olduğu söylenebilir.

### 5.4. İç Denetimin Sorumluluklarına İlişkin Ölçüm Modeli

AFA ile elde edilen faktör yapısı, DFA ile araştırma örneklemi üzerinde test edilmiştir. DFA sonuçlarına göre yapı güvenilirliği faktör yüklerinin yeterliliği, faktörlerin binişikliği veya yapıların birleşik güvenilirlik değerleri gibi ölçütler açısından değerlendirilmiştir. Ölçüm modelinde iç denetimin sorumlulukları, beş faktör altında toplanmıştır. DFA sonucunda elde edilen gözlenen 31 maddeden oluşan 5 faktörlü yapı Şekil 5.1'de verilen yol diyagramında gösterilmiştir. Yol diyagramında elipsler, yapısal modelde YRU faydaları ile ilişkileri araştırılan gizil (örtük) değişkenleri; kareler ise, ölçme aracında iç denetimin sorumluluklarını ifade eden önermeleri temsil eder. Ölçme aracında yer alan gözlenen değişkenler aracılığıyla iç denetimin Uygunluk, Bilgi Teknolojileri, Risk Yönetimi, Yönetişim ve Üstlenilmemesi Gereken Risk Yönetimi sorumluluklarını ifade eden gizil değişkenler ölçülmüştür.




Chi-Square = 770.19, df = 420, P-value = 0.00000, RMSEA = 0.058

**Şekil 5.1.** *İç Denetimin Sorumluluklarına İlişkin Yol Diyagramı*

Tablo 5.4'te sunulan gözlenen ve gizil değişkenler arasındaki ilişki katsayılarının tüm t değerleri, istatistiksel olarak (t>2,58) 0,01 düzeyinde anlamlıdır. Uygunluk Sorumlulukları faktöründe değişimi en çok açıklayan gözlenen değişken U8 (%67)'dir. Bilgi Teknolojileri Sorumlulukları gizil değişkeninde değişimi en fazla BT6 (%72) gözlenen değişkeni açıklamıştır. Risk Yönetimi faktöründe değişimi en fazla R1 ve R11 ifadeleri (%67) açıklamıştır. Yönetişim faktöründe değişimi en fazla açıklayan madde Y7 (%67) ve Üstlenilmemesi Gereken Risk Yönetimi Sorumlulukları faktöründe ise R9 (%67) olmuştur. Gizil değişkenlerin açıkladığı toplam varyansın US faktöründe %61, BTS faktöründe %61, PRS faktöründe %58, YS faktöründe %59 ve NRS faktöründe %60 olduğu belirlenmiştir.

**Tablo 5.4.** *İç Denetimin Sorumlulukları Doğrulayıcı Faktör Analizi Sonuçları*

| Faktörler / Maddeler | λ | t-değeri | $R^2$ |
|---|---|---|---|
| ***Faktör* US** | **CR:0.92; Açıklanan Varyans:0.61** | | |
| ***U3*** | 0.80 | 14.52*** | 0.640 |
| ***U5*** | 0.79 | 14.23*** | 0.624 |
| ***U7*** | 0.77 | 13.85*** | 0.593 |
| ***U8*** | 0.82 | 15.01*** | 0.672 |
| ***U9*** | 0.78 | 14.12*** | 0.608 |
| ***U10*** | 0.74 | 13.08*** | 0.548 |
| ***U12*** | 0.77 | 13.70*** | 0.593 |
| ***Faktör* BTS** | **CR:0.92; Açıklanan Varyans:0.61** | | |
| ***BT1*** | 0.73 | 12.98*** | 0.533 |
| ***BT2*** | 0.72 | 12.72*** | 0.518 |
| ***BT3*** | 0.78 | 14.38*** | 0.608 |
| ***BT5*** | 0.80 | 14.88*** | 0.640 |
| ***BT6*** | 0.85 | 16.36*** | 0.723 |
| ***BT7*** | 0.79 | 14.42*** | 0.624 |
| ***BT9*** | 0.83 | 15.78*** | 0.689 |
| ***Faktör* PRS** | **CR:0.87; Açıklanan Varyans:0.58** | | |
| ***R1*** | 0.82 | 15.19*** | 0.672 |
| ***R2*** | 0.67 | 11.34*** | 0.449 |
| ***R3*** | 0.82 | 15.00*** | 0.672 |
| ***R4*** | 0.70 | 12.17*** | 0.490 |
| ***R6*** | 0.73 | 12.71*** | 0.533 |
| ***R11*** | 0.82 | 15.19*** | 0.672 |
| ***Faktör* YS** | **CR:0.89; Açıklanan Varyans:0.59** | | |
| ***Y3*** | 0.73 | 12.71*** | 0.533 |
| ***Y4*** | 0.69 | 11.77*** | 0.476 |
| ***Y6*** | 0.79 | 14.20*** | 0.624 |
| ***Y7*** | 0.82 | 14.99*** | 0.672 |
| ***Y8*** | 0.74 | 12.91*** | 0.548 |
| ***Y9*** | 0.82 | 15.14*** | 0.672 |
| ***Faktör* NRS** | **CR:0.88; Açıklanan Varyans:0.60** | | |
| ***R7*** | 0.77 | 13.77*** | 0.593 |
| ***R8*** | 0.77 | 13.63*** | 0.593 |
| ***R9*** | 0.82 | 15.11*** | 0.672 |
| ***R10*** | 0.77 | 13.70*** | 0.593 |
| ***R13*** | 0.72 | 12.40*** | 0.518 |

***p < .01 (t>2,58)

İç denetimin sorumluluklarına ilişkin DFA'da model uygunluğunun değerlendirilmesinde kullanılan uyum iyiliği değerleri Tablo 5.5'te sunulmuştur. Ölçüm modelinin uyum iyiliği değerleri, araştırma kapsamında toplanan verinin kuramsal modele uygun olduğunu göstermektedir. Söz konusu değerlerin, iyi uyum ya da en azından kabul edilebilir sınırlar içinde olması, modelin doğrulandığını ve yapısal modelin test edilmesi aşamasına geçilebileceğini gösterir.

**Tablo 5.5.** *İç Denetimin Sorumlulukları DFA Uyum İyiliği Değerleri*

| Uyum İndeksleri | Modelin Hesaplanan Uyum Değerleri |
|---|---|
| χ 2/sd | 1.83 |
| RMSEA | 0.058 |
| RMR | 0.028 |
| SRMR | 0.059 |
| GFI | 0.83 |
| CFI | 0.93 |
| NFI | 0.85 |
| NNFI | 0.92 |

Test edilen ölçüm modelinin sonuçlarına göre, gözlenen değişkenin standartlaştırılmış faktör yükleri ve toplam açıklanan varyanslar, yapı geçerliliğinin sağlandığını doğrular niteliktedir. Birleşik güvenilirlik değerleri, geçerliliğin bir önkoşulu olan güvenilirliğin sağlandığını gösterir. Değerler ölçüm modelinin doğrulandığına işaret eder.

**Tablo 5.6.** *İç Denetimin Sorumlulukları Faktörlerinin Korelasyonu*

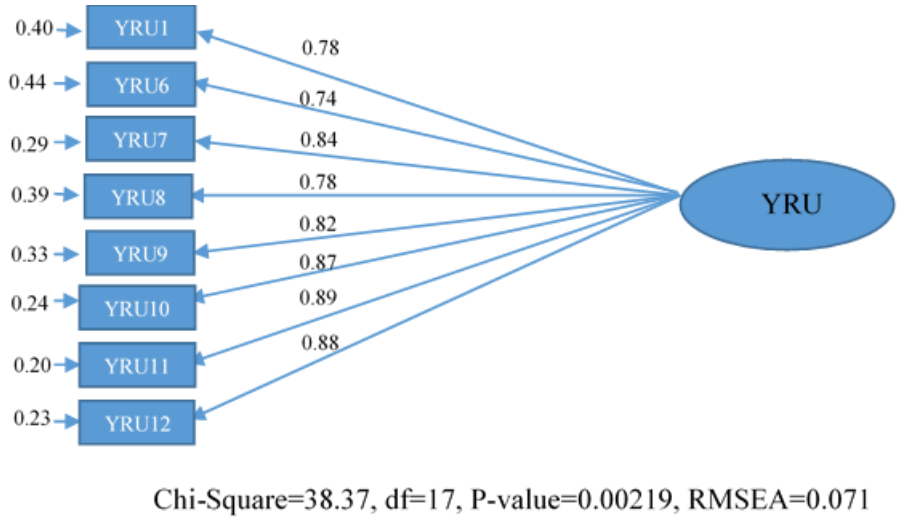
| | Yönetişim | Uygunluk | Risk (+) | Risk (-) | Bilgi Teknolojileri |
|---|---|---|---|---|---|
| Yönetişim | 1.000 | | | | |
| Uygunluk | 0.12** | 1.000 | | | |
| Risk (+) | 0.2 | 0.38** | 1.000 | | |
| Risk (-) | -0.01 | 0.07 | 0.09 | 1.000 | |
| Bilgi Teknolojileri | 0.16** | 0.16** | 0.23** | -0.2 | 1.000 |

** $p < .05$ ($t>1,96$)

İç denetimin YRU Yaklaşımı kapsamında değerlendirdiğimiz sorumluluklarına ilişkin faktörler arasındaki korelasyon Tablo 5.6'da sunulmuştur. Risk (+) ve Uygunluk gizil değişkenleri arasındaki %38'lik korelasyon, faktörler arası en yüksek korelasyon değeridir. Buna karşın Yönetişim ve iç denetimin üstlenmemesi gereken risk sorumluluklarından oluşan Risk (-) gizil değişkeni arasındaki 0.01'lik negatif korelasyon, faktörler arası en düşük korelasyon değeridir.

### 5.5. YRU Yaklaşımının Faydalarına İlişkin Ölçüm Modeli

YRU yaklaşımının faydalarına ilişkin ölçek maddeleri üzerinde AFA sonucunda ortaya çıkarılan faktör yapısı, DFA ile doğrulanmıştır. Ölçüm modeli, faktörleri oluşturan maddelerin belirlenmesi ölçütlerine göre değerlendirilmiştir. Ölçüm modelinde YRU yaklaşımının faydaları tek faktör altında toplanmıştır. Açıklanan varyans ve birleşik güvenilirlik değerleri ölçüm modelinin uygun olduğunu doğrular niteliktedir. Şekil 5.2, sekiz maddeden oluşan tek faktörlü yapıyı ifade eden yol diyagramını gösterir. Diyagramda elipsler gizil (örtük) değişkenleri, kareler ise YRU yaklaşımının faydalarına ilişkin ölçme aracında yer alan gözlenen değişkenleri temsil eder. YRU Yaklaşımının Faydaları faktörü, gözlenen değişkenler aracılığıyla ölçülmüştür.




**Şekil 5.2.** *YRU Yaklaşımının Faydalarına İlişkin Yol Diyagramı*

Tablo 5.7'de sunulan ilişki katsayılarının tüm t değerleri, istatistiksel olarak (t>2,58) 0,01 düzeyinde anlamlıdır. YRU Yaklaşımının Faydaları gizil değişkeninde, değişimi en fazla (%79) YRU11 gözlenen değişkeni açıklamıştır. Ölçme aracının varyans açıklama oranı %65'tir. Ölçme aracının en düşük (%56) açıklama oranına sahip maddesi, YRU6 gözlenen değişkenidir. Birleşik güvenilirlik katsayısı 0.95 olarak hesaplanmıştır ve iç tutarlılığın oldukça yüksek olduğunu gösterir.

**Tablo 5.7.** *YRU Yaklaşımının Faydaları Doğrulayıcı Faktör Analizi Sonuçları*

| Faktörler / Maddeler | λ | t-değeri | $R^2$ |
|---|---|---|---|
| ***Faktör* YRU** | **CR:0.95; Açıklanan Varyans:0.65** | | |
| ***YRU1*** | 0.78 | 14.31*** | 0.608 |
| ***YRU6*** | 0.75 | 13.63*** | 0.562 |
| ***YRU7*** | 0.84 | 16.12*** | 0.706 |
| ***YRU8*** | 0.78 | 14.34*** | 0.608 |
| ***YRU9*** | 0.82 | 15.41*** | 0.672 |
| ***YRU10*** | 0.87 | 17.06*** | 0.757 |
| ***YRU11*** | 0.89 | 17.86*** | 0.792 |
| ***YRU12*** | 0.88 | 17.29*** | 0.774 |

***p < .01 (t>2,58)

YRU'nun faydalarına ilişkin ölçüm modelinin uygunluğunun değerlendirilmesinde kullandığımız uyum iyiliği değerleri Tablo 5.8'de sunulmuştur. Sonuçlara göre, model araştırma örnekleminden toplanan veriye iyi uyum göstermiştir. Söz konusu değerlerin iyi uyum sınırları içinde olması, DFA sonucunda ölçüm modelinin doğrulandığını ve yapısal modelin test edilmesine geçilebileceğini gösterir.

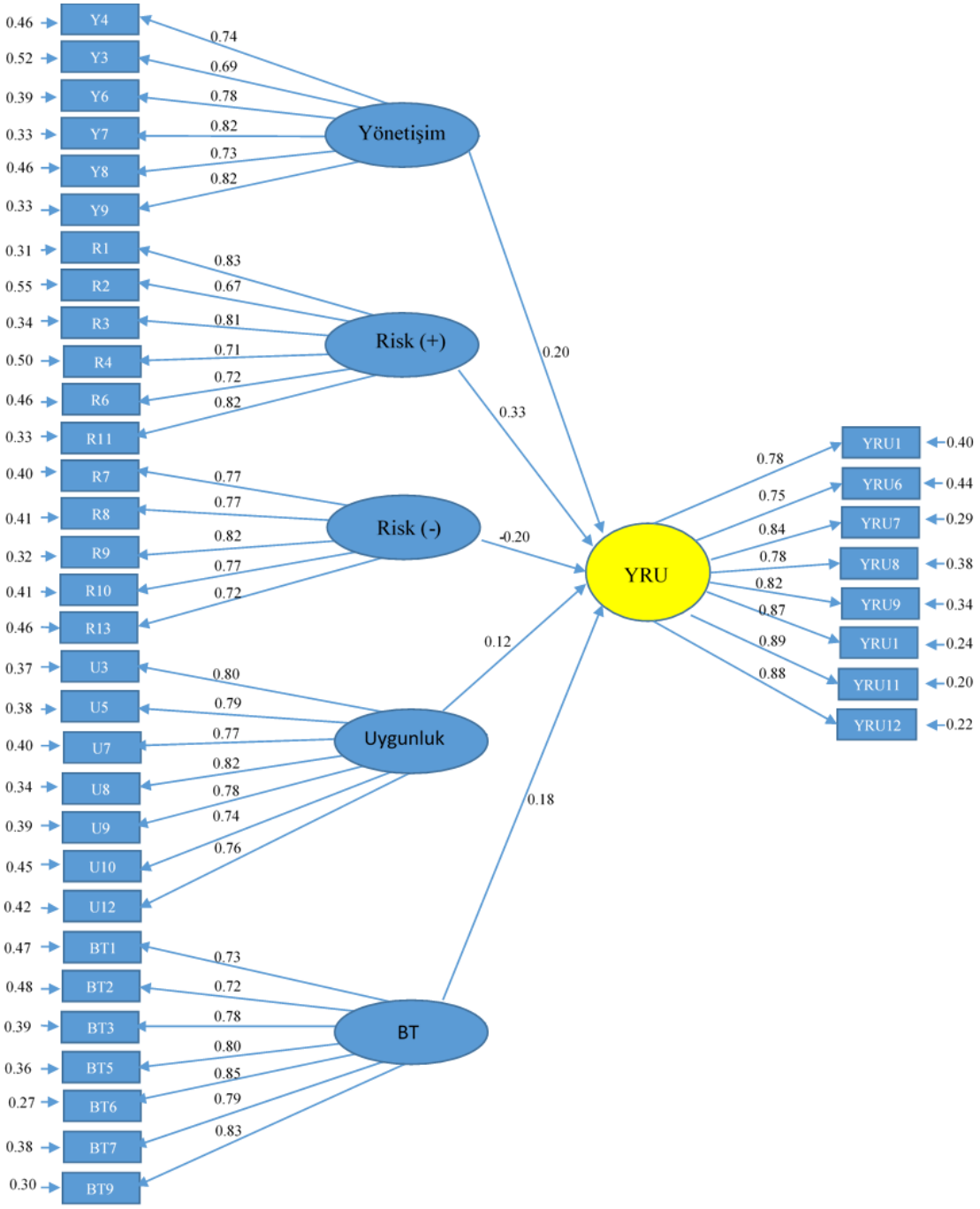
**Tablo 5.8.** *YRU Yaklaşımının Faydaları DFA Uyum İyiliği Değerleri*

| **Uyum İndeksleri** | **Modelin Hesaplanan Uyum Değerleri** |
|---|---|
| χ 2/sd | 2.257 |
| RMSEA | 0.071 |
| RMR | 0.011 |
| SRMR | 0.023 |
| GFI | 0.96 |
| CFI | 0.99 |
| NFI | 0.98 |
| NNFI | 0.98 |

Ölçüm modelinin sonuçlarına göre, gözlenen değişkenin standartlaştırılmış faktör yükleri, toplam açıklanan varyanslar ve birleşik güvenilirlik değerleri ölçüm modelinin doğrulandığına işaret eder.

### 5.6. Araştırmanın Yapısal Eşitlik Modeli

Araştırma verileri üzerinde ilk aşamada, Açımlayıcı Faktör Analizleri yürütülmüş ve veri içerisinde yer alan yapılar ortaya çıkarılmıştır. Yapısal modelin test edilmesine geçilmeden önce ölçüm modelleri test edilmiştir. AFA ile keşfedilen yapılar (faktörler) doğrultusunda oluşturulan ölçüm modellerinde, gözlenen değişkenlerin örtük değişkenleri temsil edebilme gücü, DFA ile doğrulanmıştır. Son olarak yapısal modelde dışsal (bağımsız) değişkenlerin içsel (bağımlı) değişken üzerindeki etkisi incelenmiştir. Çalışmamız kapsamında geliştirilen hipotezler, yapısal modelde test edilmiş ve içsel ve dışsal değişkenler arasındaki ilişki örüntüsü ortaya konulmuştur. Analizler neticesinde elde edilen yapısal modelin yol diyagramı Şekil 5.3'te sunulmuştur.




**Şekil 5.3.** *Yapısal Eşitlik Modeli*

YEM'in uyum iyiliği değerleri Tablo 5.9'da sunulmuştur. YEM sonuçlarına göre, model araştırma örnekleminden elde edilen veriye, bazı uyum iyiliği değerleri açısından iyi uyum, geriye kalan uyum iyiliği değerleri açısından ise kabul edilebilir uyum göstermiştir. Söz konusu değerlerin kabul edilebilir uyum sınırları içinde ya da en azından sınırlara çok yakın olması, araştırmamızın yapısal modelinin kabul edilebilir bir model olduğunu gösterir.

**Tablo 5.9.** *Yapısal Modelin Uyum İyiliği Değerleri*

| Uyum İndeksleri | Modelin Hesaplanan Uyum Değerleri |
|---|---|
| $\chi$ 2/sd | 1.637 |
| RMSEA | 0.051 |
| RMR | 0.027 |
| SRMR | 0.058 |
| GFI | 0.81 |
| CFI | 0.93 |
| NFI | 0.84 |
| NNFI | 0.92 |

Beş faktörden oluşan iç denetimin sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini değerlendirmek için yapısal modelin değişkenleri arasındaki ilişki katsayıları incelenmelidir. Hipotezlere konu olan değişkenler arasındaki ilişkinin yönü, standartlaştırılmış yükler, t değerleri ve hipotez testlerinin sonuçları Tablo 5.10'da toplu olarak gösterilmiştir.

**Tablo 5.10.** *Yapısal Modelin Hipotez Testi Sonuçları*

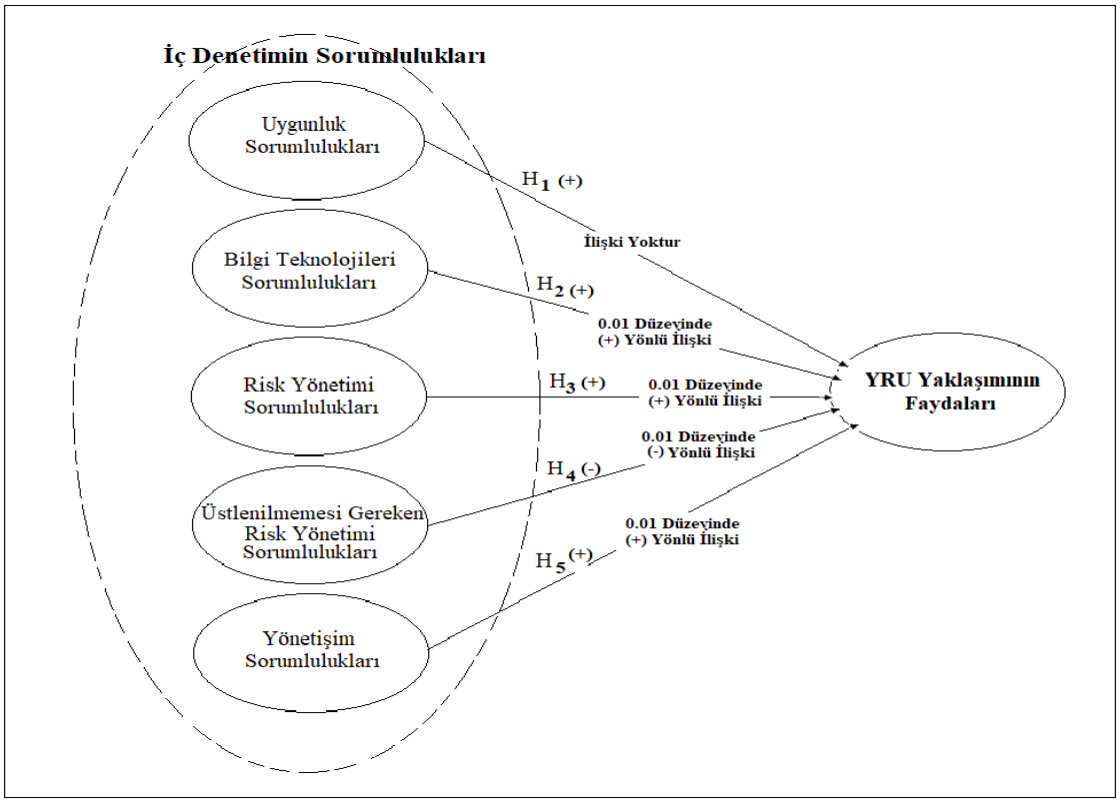
| Hipotezler | Standart Yükler | t- değeri | $R^2$ | Sonuç |
|---|---|---|---|---|
| **US → YRU** | 0.12 | 1.85 | 0.014 | $H_1$Red |
| **BTS → YRU** | 0.18 | 2.81*** | 0.032 | $H_2$Kabul |
| **PRS → YRU** | 0.33 | 4.7*** | 0.109 | $H_3$Kabul |
| **YS → YRU** | 0.2 | 3.26*** | 0.040 | $H_4$Kabul |
| **NRS → YRU** | -0.2 | -3.3*** | 0.040 | $H_5$Kabul |

***p < .01 (t>2,58)

Araştırmamız kapsamında test edilen modelin sonuçları şöyle formüle edilebilir: YRU= 0.20xYS + 0.33xPRS - 0.20NRS + 0.18xBTS. Araştırma modelinden elde edilen yapısal eşitlik, dört bağımsız (dışsal-egzojen) değişkenin bağımlı (içsel-endojen) değişken üzerindeki etkisini tanımlar.

Hipotezlerin ifade ettiği ilişki katsayılarının t istatistik değerleri $H_2$-$H_3$-$H_4$ ve $H_5$ hipotezleri için (t>2,58) 0,01 seviyesinde istatistiksel olarak anlamlıdır. Tablo 5.14'teki

değerler yorumlandığında, iç denetimin sorumlulukları ile YRU yaklaşımının faydaları arasında (uygunluk sorumlulukları dışında) istatistiksel olarak anlamlı ilişkiler keşfedilmiştir. İç denetimin bilgi teknolojileri, risk ve yönetişim sorumlulukları ile YRU yaklaşımından beklenen faydalar arasında (t>2,58) 0,01 seviyesinde pozitif yönlü ilişki gözlenmiştir. Uygunluk sorumlulukları ile YRU yaklaşımının faydaları arasında ise, (t>1,96) 0,05 anlamlılık seviyesinde ilişki bulunamamıştır. İç denetimin üstlenmemesi gereken risk sorumlulukları ile YRU yaklaşımının faydaları arasında ise (t>2,58) 0,01 seviyesinde negatif yönlü ilişki gözlenmiştir. Yapısal modelden elde edilen bulgular, iç denetimin bilgi teknolojileri, risk ve yönetişim sorumluluklarında 1 birimlik artışın YRU yaklaşımının faydaları üzerinde sırasıyla 0.18, 0.33 ve 0.20 birimlik bir artışa neden olacağını gösterir. Diğer taraftan bulgulara göre, iç denetimin üstlenmemesi gereken risk sorumluluklarında 1 birimlik artış, YRU yaklaşımının faydaları üzerinde 0,20 birim azalmaya neden olur. Yapısal modelden elde edilen sonuçlar doğrultusunda, öngörülen dört hipotez kabul edilmiştir. Kabul edilen kuramsal model Şekil 5.4'te verilmiştir.




**Şekil 5.4.** *Kabul Edilen Kuramsal Model*

### 5.7. İç Denetimin Sorumluluklarına İlişkin Karşılaştırmalı Analizler

Çalışmanın amaçları doğrultusunda geliştirilen hipotezleri test etmek amacıyla öncelikle iç denetimin sorumlulukları hakkında olması gereken durum ile uygulamadaki duruma ilişkin iç denetçilerin görüşleri eşleştirilmiş örneklemler t testi ile analiz edilmiştir. Daha sonra iç denetim hizmetlerini değerlendirebileceği öngörülen taraflar olarak tanımladığımız, işletme yöneticileri ve bağımsız denetçilerin iç denetim sorumlulukları hakkında olması gereken ile uygulamadaki duruma ilişkin görüşleri eşleştirilmiş örneklemler t testiyle karşılaştırılmıştır. Ayrıca iki gruba ilişkin (iç denetçiler ve iç denetim hizmetlerinden doğrudan faydalanan taraflar) olması gereken duruma ve uygulamadaki duruma ilişkin görüşler ayrı ayrı bağımsız örneklemler t testiyle değerlendirilmiştir. Son olarak, iki grubun YRU yaklaşımının faydaları hakkındaki görüşleri bağımsız örneklemler t testiyle analiz edilmiştir.

#### 5.7.1. İç Denetçilerin Olması Gereken Duruma ve Uygulamaya İlişkin Görüşleri

Çalışmamızın amaçları doğrultusunda iç denetçilerin, iç denetimin sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşlerini karşılaştırmak için $H_6$ ve alt hipotezler geliştirilmiştir.

Eşleştirilmiş örneklemler t testi, aynı grubun iki farklı soruya (çalışmamızda olması gereken ve uygulamada) verdiği yanıtlar değerlendirilirken kullanılabilir. Soruların aynı ölçek tipiyle (çalışmamızda beşli Likert) kurgulanması gerekir. $H_6$ Hipotezinin alt hipotezleri, eşleştirilmiş örneklemler t testiyle analiz edilmiştir. Sonuçlar Tablo 5.11'de sunulmuştur:

**Tablo 5.11.** *İç Denetçilerin Görüşlerinin Eşleştirilmiş Örneklemler t Testi Sonuçları*

| Hipotez | Ölçüm | n | $\bar{X}$ | $\Delta\bar{X}$ | ΔSS | SD | t | Etki Büyüklüğü (Cohen d) |
|---|---|---|---|---|---|---|---|---|
| $H_{6a}$ | Olması Gereken<br>Uygulamada | 247 | 4,00<br>4,01 | -,006 | ,092 | 246 | -0,99 | |
| $H_{6b}$ | Olması Gereken<br>Uygulamada | 247 | 4,45<br>4,26 | ,191 | ,271 | 246 | 11,11*** | 0.405 |
| $H_{6c}$ | Olması Gereken<br>Uygulamada | 247 | 4,33<br>4,32 | ,010 | ,102 | 246 | 1,56 | |
| $H_{6d}$ | Olması Gereken<br>Uygulamada | 247 | 4,13<br>4,16 | -,023 | ,206 | 246 | -1,75 | |
| $H_{6e}$ | Olması Gereken<br>Uygulamada | 247 | 2,14<br>2,16 | -,010 | ,122 | 246 | -1,25 | |

***p < .01 (t>2,58)

İç denetçilerin iç denetimin sorumlulukları hakkında teoriye ve uygulamaya ilişkin görüşleri arasındaki farkı değerlendirmek için eşleştirilmiş örneklemler t testi yürütülmüştür. İç denetçilerin risk, uygunluk, üstlenilmemesi gereken risk ve yönetişim sorumluluklarına ilişkin görüşleri arasında anlamlı farklılık belirlenememiştir. Sadece bilgi teknolojileri sorumluluklarına ilişkin görüşlerde teoriden (μ=4,45) uygulamaya (μ=4,26) istatistiksel olarak anlamlı bir düşüş keşfedilmiştir; *t(246)*= 11,11; p<0.001; d=0,40. Hesaplanan etki büyüklüğü değeri, orta düzey etkiyi gösterir.

### 5.7.2. Diğer Katılımcıların Olması Gereken Duruma ve Uygulamaya İlişkin Görüşleri

İç denetim hizmetlerini değerlendirebileceği öngörülen taraflar olarak tanımladığımız, işletme yöneticileri ve bağımsız denetçilerin iç denetim sorumlulukları hakkında olması gereken duruma ve uygulamadaki duruma ilişkin görüşlerini karşılaştırmak için $H_7$ hipotezi geliştirilmiştir.

$H_7$ ve alt hipotezlerinin test edilmesi için eşleştirilmiş örneklemler t testi yürütülmüştür. Testin sonuçları Tablo 5.12'de sunulmuştur:

**Tablo 5.12.** *Diğer Katılımcıların Görüşlerinin Eşleştirilmiş Örneklemler t Testi Sonuçları*

| Hipotez | Ölçüm | n | X̄ | ΔX̄ | ΔSS | SD | t | Etki Büyüklüğü (Cohen d) |
|---|---|---|---|---|---|---|---|---|
| $H_{7a}$ | Olması Gereken | 168 | 4,18 | ,639 | ,559 | 167 | 14,80*** | 1.362 |
| | Uygulamada | | 3,54 | | | | | |
| $H_{7b}$ | Olması Gereken | 168 | 4,46 | ,812 | ,588 | 167 | 17,90*** | 1.492 |
| | Uygulamada | | 3,64 | | | | | |
| $H_{7c}$ | Olması Gereken | 168 | 4,34 | ,720 | ,566 | 167 | 16,50*** | 1.468 |
| | Uygulamada | | 3,62 | | | | | |
| $H_{7d}$ | Olması Gereken | 168 | 4,26 | ,658 | ,486 | 167 | 17,55*** | 1.384 |
| | Uygulamada | | 3,60 | | | | | |
| $H_{7e}$ | Olması Gereken | 168 | 2,15 | -,005 | ,529 | 167 | -0,15 | |
| | Uygulamada | | 2,16 | | | | | |

***p < .01 (t>2,58)

İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı grubunun iç denetimin sorumlulukları hakkında teoriye ve uygulamaya ilişkin görüşleri arasındaki farkı değerlendirmek için eşleştirilmiş örneklemler t testi yürütülmüştür. Uygunluk, bilgi teknolojileri, risk ve yönetişim sorumluluklarıyla ilgili görüşlerde istatistiksel olarak anlamlı farklılık keşfedilirken, üstlenilmemesi gereken risk sorumluluklarıyla ilgili görüşlerde farklılık olmadığı anlaşılmıştır. Uygunluk sorumluluklarına ilişkin görüşlerde

teoriden (μ=4,18) uygulamaya (μ=3,54) anlamlı bir düşüş keşfedilmiştir; *t(167)*=14,80; p<0.001; d=1,36. Bilgi teknolojileri sorumlulukları faktöründe teori (μ=4,45) ve uygulama (μ=3,64) arasında anlamlı bir farklılık (*t(167)*=17,90; p<0.001; d=1,49) bulunmuştur. Risk faktöründe teori (μ=4,33) ve uygulama (μ=3,61) ile ilgili görüşler arasında anlamlı farklılık (*t(167)*=16,50; p<0.001; d=1,46) vardır. Son olarak yönetişim sorumluluklarında teori (μ=4,26) ve uygulama (μ=3,60) ile ilgili görüşler farklılık (*t(167)*=17,55; p<0.001; d=1,34) gösterir. Hesaplanan değerler, anlamlı farklılık bulunan dört test için etki büyüklüğünün yüksek olarak yorumlanması gerektiğini gösterir.

### 5.7.3. Olması Gereken Duruma İlişkin Görüşlerin Karşılaştırılması

Birçok araştırma, bir değişken ile ilgili araştırma kapsamına alınan grupların, bağımlı değişkene ait ölçümlerinin karşılaştırılmasını amaçlar. Gruplar arasında tespit edilen farkların istatistiksel olarak anlamlılığı, hipotez testleriyle değerlendirilir. Araştırmamız kapsamında, iç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı gruplarının iç denetimin sorumlulukları hakkında olması gereken durum ile ilgili görüşlerini karşılaştırmak için $H_8$ hipotezi geliştirilmiştir.

$H_8$ ve alt hipotezlerinin test edilmesi için bağımsız örneklemler t testi yürütülmüştür. Bağımsız örneklemler t testi, iki ilişkisiz katılımcı grubunun ortalamaları arasındaki farklılığın istatistiksel olarak anlamlılığını test eder. Testin sonuçları Tablo 5.13'te sunulmuştur:

**Tablo 5.13.** *Olması Gereken Duruma İlişkin Görüşlerin Bağımsız Örneklemler t Testi Sonuçları*

| Hipotez | Grup | n | $\bar{X}$ | $\Delta\bar{X}$ | SS | SD | t | Etki Büyüklüğü (Cohen d) |
|---|---|---|---|---|---|---|---|---|
| $H_{8a}$ | İç Denetçiler | 247 | 4,01 | ,175 | ,627 | 413 | 3,21*** | 0.312 |
| | Diğer Katılımcılar* | 168 | 4,18 | | ,480 | | | |
| $H_{8b}$ | İç Denetçiler | 247 | 4,45 | ,003 | ,511 | 413 | ,06 | |
| | Diğer Katılımcılar* | 168 | 4,46 | | ,423 | | | |
| $H_{8c}$ | İç Denetçiler | 247 | 4,33 | ,009 | ,498 | 413 | ,19 | |
| | Diğer Katılımcılar* | 168 | 4,34 | | ,409 | | | |
| $H_{8d}$ | İç Denetçiler | 247 | 4,13 | ,133 | ,474 | 413 | 2,93*** | 0.291 |
| | Diğer Katılımcılar* | 168 | 4,27 | | ,441 | | | |
| $H_{8e}$ | İç Denetçiler | 247 | 2,14 | ,003 | ,720 | 413 | ,047 | |
| | Diğer Katılımcılar* | 168 | 2,15 | | ,608 | | | |

*Bağımsız Denetçiler ve İşletme Yöneticileri ***p < .01 (t>2,58)

Bağımsız örneklemler t testinde iki farklı gruptan elde edilen verilerin varyanslarının eşitliği değerlendirilmelidir. Bunun için Levene testinin sonuçları incelenmelidir. SPSS'te Levene testiyle elde edilen anlamlılık değeri 0,05'ten büyükse, varyansların eşitliği önermesinin ihlal edilmediği sonucunda varılır ve bağımsız örneklemler t testi için varyanslar eşit varsayılmıştır satırında yer alan t ve p değerleri geçerli kabul edilir. Tersi durumda ise, varyansların eşit olmadığı anlaşılır ve varyansların eşit olmadığı varsayılmıştır satırında yer alan t ve p değerleri geçerli kabul edilir (Pallant, 2016, s. 268). Levene testinden elde ettiğimiz sonuçlar verilerin varyanslarının eşit varsayılmaması gerektiğini gösterir. Tablo 5.13'te sunulan t ve p değerleri, Levene testi sonuçlarına uygun şekilde sunulmuştur.

İşletme yöneticileri ve bağımsız denetçilerden oluşan katılımcılar ile iç denetçilerin, iç denetimin sorumlulukları hakkında olması gereken duruma yönelik görüşleri arasındaki farkı değerlendirmek amacıyla yürütülen bağımsız örneklemler t testlerinin sonuçlarına göre risk, bilgi teknolojileri ve üstlenilmemesi gereken risk sorumlulukları ile ilgili görüşlerin ortalamaları arasında istatistiksel olarak anlamlı farklılık yoktur. Diğer taraftan iç denetimin uygunluk ve yönetişim sorumluluklarında ortalamalar arasında istatistiksel olarak anlamlı bir farklılık keşfedilmiştir. İç denetimin uygunluk sorumlulukları ile ilgili iç denetçilerin görüşlerinin ortalamaları ($\mu$=4,01) diğer katılımcılardan ($\mu$=4,18) anlamlı şekilde ($t(413)$=3,21; p<0.001; d=0,31) düşüktür. Yine iç denetimin yönetişim sorumlulukları ile ilgili iç denetçilerin görüşlerinin ortalamaları ($\mu$=4,13) diğer katılımcılardan ($\mu$=4,26) anlamlı şekilde ($t(413)$=2,93; p<0.001; d=0,29) düşüktür. Hesaplanan istatistikler, etki büyüklüğünün düşük ile orta düzey arasında olduğunu gösterir.

### 5.7.4. Uygulamaya İlişkin Görüşlerin Karşılaştırılması

Araştırmamızın amaçları doğrultusunda gruplar arasında tespit edilen farkların istatistiksel olarak anlamlılığı, hipotez testleriyle değerlendirilmiştir. İç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan katılımcı gruplarının iç denetimin sorumlulukları hakkında uygulamadaki durum ile ilgili görüşlerini karşılaştırmak için $H_9$ hipotezi geliştirilmiştir.

$H_9$ ve alt hipotezlerinin test edilmesi için iki ilişkisiz katılımcı grubunun ortalamaları arasındaki farklılığın istatistiksel olarak anlamlılığını ölçen bağımsız

örneklemler t testi yürütülmüştür. Bağımsız örneklemler t testi sonuçları Tablo 5.14'te sunulmuştur:

**Tablo 5.14.** *Uygulamaya İlişkin Görüşlerin Bağımsız Örneklemler t Testi Sonuçları*

| Hipotez | Grup | n | $\bar{X}$ | $\Delta\bar{X}$ | SS | SD | t | Etki Büyüklüğü (Cohen d) |
|---|---|---|---|---|---|---|---|---|
| $H_{9a}$ | İç Denetçiler | 247 | 4,01 | ,47048 | ,591 | 413 | 9,12*** | 0.889 |
| | Diğer Katılımcılar* | 168 | 3,54 | | ,457 | | | |
| $H_{9b}$ | İç Denetçiler | 247 | 4,26 | ,61772 | ,431 | 413 | 10,90*** | 1.129 |
| | Diğer Katılımcılar* | 168 | 3,64 | | ,643 | | | |
| $H_{9c}$ | İç Denetçiler | 247 | 4,32 | ,70147 | ,476 | 413 | 13,71*** | 1.350 |
| | Diğer Katılımcılar* | 168 | 3,62 | | ,560 | | | |
| $H_{9d}$ | İç Denetçiler | 247 | 4,16 | ,54841 | ,438 | 413 | 11,71*** | 1.155 |
| | Diğer Katılımcılar* | 168 | 3,61 | | ,508 | | | |
| $H_{9e}$ | İç Denetçiler | 247 | 2,15 | ,00075 | ,691 | 413 | ,011 | |
| | Diğer Katılımcılar* | 168 | 2,16 | | ,616 | | | |

*Bağımsız Denetçiler ve İşletme Yöneticileri ***p < .01 (t>2,58)

Bağımsız örneklemler t testinde grup verilerinin varyanslarının eşitliğini kontrol etmek için Levene testi sonuçları değerlendirilmelidir. Levene testinden elde edilen sonuçlar; risk, yönetişim ve üstlenilmemesi gereken risk sorumluluklarına ilişkin grup verilerinin varyanslarının eşit olduğunu göstermiştir. Levene testi sonuçlarına göre bağımsız örneklemler t testinde uygun t ve p değerleri dikkate alınmış ve Tablo 5.14'te raporlanmıştır.

İç denetçiler ile işletme yöneticileri ve bağımsız denetçilerden oluşan grubun, iç denetimin sorumlulukları hakkında uygulamadaki duruma yönelik görüşleri arasında yürütülen bağımsız örneklemler t testi sonuçlarına göre üstlenilmemesi gereken risk sorumlulukları ile ilgili görüşlerin ortalamaları istatistiksel olarak farklılık göstermemiştir. İç denetimin araştırma kapsamında ele aldığımız diğer sorumlulukları ile ilgili olarak iki grubun uygulamaya yönelik görüşlerinin ortalamaları arasında ise, anlamlı bir farklılık tespit edilmiştir. İç denetimin sorumluluklarına yönelik ortalamalar arasındaki tüm farklılıkların iç denetçi lehine olduğu belirlenmiştir. İç denetimin uygunluk sorumlulukları ile ilgili iç denetçilerin görüşlerinin ortalamaları (μ=4,01) diğer gruptan (μ=3,54) anlamlı şekilde (*t(413)*=9,12; p<0.001; d=0,89) yüksektir. Aynı şekilde bilgi teknolojileri sorumlulukları ile ilgili iç denetçilerin görüşlerinin ortalamaları

(μ=4,26) diğer gruptan (μ=3,64) anlamlı şekilde (*t(413)*=10,90; p<0.001; d=1,13) yüksektir. Yine iç denetçilerin risk sorumluluklarına yönelik görüşlerinin ortalamaları (μ=4,32) diğer gruptan (μ=3,62) anlamlı şekilde (*t(413)*=13,71 p<0.001; d=1,35) yüksektir. Son olarak iç denetçilerin yönetişim sorumluluklarına yönelik görüşlerinin (μ=4,15) diğer grubun ortalamalarından (μ=3,61) anlamlı şekilde (*t(413)*=11,71 p<0.001; d=1,15) yüksek olduğu belirlenmiştir. Ayrıca, hesaplanan istatistikler, ortalamalar arasında tespit edilen istatistiksel olarak anlamlı farklılıkların etki büyüklüklerinin yüksek düzeyde olduğunu göstermiştir.

### 5.7.5. YRU Yaklaşımının Faydalarına İlişkin Görüşlerin Karşılaştırılması

Araştırmamızın amaçları doğrultusunda iç denetçiler ile bağımsız denetçiler ve işletme yöneticilerden müstakil grupların YRU yaklaşımından beklenen faydaya yönelik görüşleri arasında istatistiksel olarak anlamlı farklılık olup olmadığı araştırma kapsamında geliştirilen hipotezler aracılığıyla test edilmiştir. YRU yaklaşımının faydaları ile ilgili görüşleri karşılaştırmak amacıyla $H_{10}$ hipotezi geliştirilmiştir.

$H_{10}$ hipotezi, iki farklı ilişkisiz katılımcı grubunun ortalamaları arasındaki farklılığın istatistiksel olarak anlamlılığını ölçen bağımsız örneklemler t testi ile test edilmiştir. YRU yaklaşımının faydalarına yönelik ölçümlerin, bağımsız örneklemler t testi sonuçları Tablo 5.15'te sunulmuştur:

**Tablo 5.15.** *YRU Yaklaşımının Faydalarına İlişkin Görüşlerin Bağımsız Örneklemler t Testi Sonuçları*

| Hipotez | Grup | n | $\bar{X}$ | $\Delta\bar{X}$ | SS | SD | t | Etki Büyüklüğü (Cohen d) |
|---|---|---|---|---|---|---|---|---|
| $H_{10}$ | İç Denetçiler | 247 | 4,37 | ,173 | ,601 | 413 | 3,52*** | 0.339 |
| | Diğer Katılımcılar* | 168 | 4,20 | | ,403 | | | |

*Bağımsız Denetçiler ve İşletme Yöneticileri ***p < .01 (t>2,58)

Bağımsız örneklemler t testinde grup verilerinin varyanslarının eşitliğini sınamak için Levene testi yürütülmüştür. Sonuçlar varyansların eşit olmadığını göstermiştir ve bağımsız örneklemler t testinin değerlendirilmesinde uygun değerler dikkate alınmıştır.

İç denetçilerden oluşan grubun YRU yaklaşımının faydalarına yönelik görüşleri ile bağımsız denetçiler ve işletme yöneticilerinden oluşan grubun görüşlerinin ortalamaları arasında bağımsız örneklemler t testi sonuçlarına göre iç denetçiler lehine istatistiksel olarak anlamlı bir farklılık belirlenmiştir. İç denetçilerden oluşan grubun görüşlerinin

ortalamaları (μ=4,01) diğer grubun ortalamalarından (μ=3,54) istatistiksel olarak anlamlı bir şekilde (*t(413)*=9,12; p<0.001; d=0,34) yüksektir. Ancak hesaplanan istatistikler, ortalamalar arasında tespit edilen anlamlı farkın etki büyüklüğünün küçük ve orta düzey arasında olduğunu göstermektedir.

## 5.8. Açık Uçlu Soru Analizi

Katılımcılardan veri toplama formunda, iki açık uçlu soruya cevap vermeleri istenmiştir. Açık uçlu sorular ile katılımcılardan, 'işletmelerinde uyguladıkları risk yönetimi modeli' ve 'veri toplama formunu doldurmadan önce YRU yaklaşımı hakkında bilgi sahibi olup olmadıkları' konusunda yanıt vermeleri istenmiştir. YRU yaklaşımı hakkında bilgi sahibi olunup olunmadığına verilen cevaplar, Tablo 5.16'da özetlenmiştir.

**Tablo 5.16.** *Örneklemin YRU Hakkında Bilgi Düzeyi*

| | **YRU Hakkında Bilgi Sahibi mi?** | | |
|---|---|---|---|
| **Unvan** | **Evet** | **Hayır** | **Cevap Yok** |
| ***İç Denetçi (n=247)*** | 136 | 89 | 22 |
| ***Bağımsız Denetçi (n=96)*** | 42 | 53 | 1 |
| ***İşletme Yöneticisi (n=72)*** | 16 | 54 | 2 |
| ***Toplam (n=415)*** | **194, %47** | **196, %47** | **25, %6** |

İşletmelerinde uyguladıkları risk yönetim modelinin yanıtının arandığı soruya, doğal olarak bağımsız denetçilerin neredeyse tamamının yanıt vermediği belirlenmiştir. Ayrıca Likert tipi ölçekle hazırlanan sorular ile karşılaştırıldığında, her iki soruyu cevapsız bırakanların sayısının fazlalığı dikkat çekmiştir. İç denetçilerin ve işletme yöneticilerinin işletmelerinde uyguladıkları risk yönetim modeli sorusuna verdikleri yanıtlar, Tablo 5.17'de özetlenmiştir.

**Tablo 5.17.** *İşletmenin Risk Yönetim Modeli Sorusuna Verilen Yanıtlar*

| | **İşletmenin Risk Yönetim Modeli** | | | | | | **Cevap Yok** |
|---|---|---|---|---|---|---|---|
| **Unvan** | ***COSO*** | ***ISO31000*** | ***YRU*** | ***BDDK*** | ***Kendi Modeli*** | ***COBIT*** | |
| ***İç Denetçi (n=247)*** | 142 | 24 | 8 | 8 | 6 | 3 | 56 |
| ***İşletme Yöneticisi (n=72)*** | 28 | 25 | 4 | 0 | 2 | 1 | 10 |
| ***TOPLAM (n=319)*** | **170, %53** | **49, %15** | **12, %4** | **8, %3** | **8, %3** | **4, %1** | **66, %21** |

# 6. SONUÇ, TARTIŞMA, DEĞERLENDİRME VE ÖNERİLER

Bu bölümde YRU yaklaşımı ve iç denetim ilişkisi tartışılmış, araştırma bulguları değerlendirilmiş, çalışmanın sonuçlarına yer verilmiş ve gelecekte yapılacak çalışmalar için öneriler sunulmuştur.

## 6.1. YRU Yaklaşımı ve İç Denetim İlişkisine Yönelik Tartışma ve Değerlendirmeler

Giderek karmaşıklaşan günümüzün işletme dünyası, öncelikli olarak faaliyetler üzerinde önlem almaya odaklanan iç denetim fonksiyonunu, işletme performansının geliştirilmesine destek sağlayan daha proaktif bir forma dönüştürmüştür. Dünya klasındaki bir iç denetim birimi, sadece bilgi sağlamaktan çok daha fazlasını yapar. İşletmelerin karşılaştıkları zorlukları, kavramları ve trendleri tanıma konusunda yönetime destek sağlamak için gereken bilgiyi analiz etme, sentezleme ve yorumlama gibi görevleri de üstlenir. İç denetçiler, YRU yaklaşımını güvence faaliyetlerinde verimliliği artıran ve daha güçlü işletme performansı sağlayan bir girişim olarak dikkate almak zorundadır. YRU yaklaşımı risk, kontrol, uygunluk ve iç denetim gibi güvence faaliyetlerinin birbirleriyle ve iş performansıyla ilişkilerini ve bağlantılarını öne çıkaran, söz konusu faaliyetlerin stratejik yönetimini sağlayan yeni bir yönetişim çerçevesidir. İç denetçilerin organizasyonları içinde rolünü, büyük ölçüde değiştirme ve zenginleştirme potansiyeline sahip bir yaklaşımdır. İç denetim, YRU yaklaşımının savunduğu farklı fonksiyonlar arasında işbirliği ve eşgüdümün sağlanması ve faaliyetler arasında bağlantı ve örtüşmelerin belirlenmesi açısından eşsiz bir pozisyona sahiptir. Çünkü iç denetçiler, güvence ve danışmanlık hizmetleri çerçevesinde işletmelerinin tüm fonksiyonlarını inceleme ve faaliyetlerini değerlendirme fırsatına sahiptir. Bu bağlamda, iç denetçiler, YRU yaklaşımının geliştirilmesi konusunda üst yönetimin en önemli destekçileridir.

YRU yaklaşımının işletmede oturtulmasını sağlamak amacıyla iç denetçilerin üzerlerindeki sorumluluğu gerektiği gibi yerine getirebilmeleri için bir takım bilgi ve becerileri öğrenmeye çalışmaları ve kendilerini bu girişime hazırlamaları gerekir. YRU yaklaşımının uygulamaya geçirilmesi basit bir projenin uygulanmasından çok daha köklü bir değişimdir ve iç denetçiler bu değişimi anlayacak, uygulayacak ve işletme içinde uygulanmasını sağlayacak yöneticilik yeteneğini kazanmalıdırlar. Diğer taraftan, birçok fonksiyonun birlikte çalışmasını ve koordinasyonu savunan YRU yaklaşımının benimsenmesinde, iç denetçiler uygulanması amaçlanan birbirinden çok farklı alanları

kapsayan çerçeveleri keşfetmeli ve anlamalıdırlar. Bununla beraber, iç denetçiler işletme içi ve dışı uygunluk ve kurumsal yönetişim gereklilikleri konusunda bilgi sahibi olmalıdırlar. Son olarak, YRU yaklaşımının teknolojik altyapısının geliştirilmesi amacıyla, iç denetim fonksiyonu, en azından BT uzmanlarını yönlendirebilecek seviyede teknoloji bilgisine sahip olmalıdır. Bu konuda, denetim ekiplerinde teknolojik araçlar ve yenilikler konusunda uzman bir iç denetçi bulundurulması doğru bir çözümdür.

Araştırmamız kapsamında elde edilen veriler üzerinde, iç denetimin sorumluluklarının beş faktörlü bir yapı olduğu belirlenmiştir. İç denetimin yönetişim, risk, uygunluk ve teknolojiye ilişkin sorumlulukları olarak isimlendirilen likert ölçeğiyle kurgulanan önermelere iç denetçilerin verdikleri yanıtların ortalamalarının sırasıyla 4,13 – 4,33 – 4,01 – 4,45 olduğu belirlenmiştir. Bağımsız denetçilerden ve işletme yöneticilerinden oluşan diğer katılımcıların yanıtlarının ortalamaları ise sırasıyla 4,27 – 4,34 – 4,18 – 4,46 olmuştur. Söz konusu bulgular, araştırma örneklemimizin iç denetçilerin sorumlulukları hakkındaki önermeleri doğruladıklarını göstermiştir. İç denetçilerin ve diğer katılımcıların görüşlerine göre, iç denetim fonksiyonu organizasyonlarında yönetişim, risk, uygunluk ve teknolojiye ilişkin güvence ve YRU yaklaşımının geliştirilmesi için gerekli olan katılımcı rolüyle desteklenen danışmanlık hizmetlerinden oluşan sorumlulukları üstlenmelidir.

İç denetçiler, YRU yaklaşımında çift yönlü bir rol üstlenirler. İç denetçiler, bir yandan aynı zamanda YRU yaklaşımının katılımcılarından biri olarak en iyi uygulamalar konusunda diğer birimlere ve yönetime danışmanlık hizmetini sunarken, diğer taraftan işletmenin yönetişim, risk yönetimi ve kontrol faaliyetlerinin etkinliği üzerine güvence sağlamaktan sorumludurlar. İç denetçiler, bu çift yönlü rolü birimlerinin organizasyon şemasındaki özel statüsüne bağlı olarak yönetirler. Bazı durumlarda, iç denetim bir YRU projesinin başlatılması ve faydalarının çalışanlar tarafından anlaşılması konusunda üst yönetime destek sunan bir görev üstlenebilir. Diğer taraftan, eğer farklı risk ve kontrol birimleri bu görevi üstlenirse, iç denetim, hem işletme birimlerine hem de üst yönetime tavsiyeler sunan nesnel bir ses olma görevini üstlenmelidir.

İç denetçilerin yönetime tavsiyeler sunarken dikkate alması gereken belki de en önemli konu, iç denetimin YRU faaliyetleri geliştirilirken veya YRU yaklaşımının savunduğu iç kontroller ve risk yönetimi eylemleri oluşturulurken yönetsel sorumluluk üstlenmemesidir. Ayrıca, işletme faaliyetleri ve fonksiyonları YRU yaklaşımının

savunduğu felsefeye uygun hale getirilmeye çalışılırken, iç denetim biriminin organizasyon şemasında bağımsızlığını savunacak şekilde konumlandırılması gerekmektedir. IIA, YRU yaklaşımının geliştirilmesinde risk ve kontrol fonksiyonlarının oluşturulması aşamasında iç denetim fonksiyonunun gerekli sorumlulukları üstlenmesi ve YRU faaliyetlerinde etkili iç denetim faaliyetinin yürütülmesi için pozisyon raporları aracılığıyla iç denetçilere önerdiği üç hatlı savunma modelinin, mesleğin bağımsızlığının korunması ve iç denetçilerin objektif hareket edebilmesi açısından olağanüstü etkili olduğunu vurgulamıştır. Üç hatlı savunma modeli, yönetim ve denetim fonksiyonları ile ikinci hatta konumlandırılan risk ve kontrol fonksiyonlarının, işletme çevresinde bulunan risklere karşı eşgüdüm ve işbirliği içerisinde tepki göstermesini sağlayan örgütsel çerçeveyi ve sorumluluk sınırlarını belirler.

Üç hatlı savunma modelinin amacı, risk yönetimi, kontrol ve güvence faaliyetlerinde, her fonksiyonun görev ve sorumluluklarına uygun şekilde koordinasyonunu sağlamaktır. Bu faaliyetlerin işbirliği içinde yürütülmesi, işletmeye örgütsel yapının tüm seviyelerinde daha fazla şeffaflık ve operasyonel verimlilik gibi birçok fayda sağlar. Üç hatlı savunma modelinde, iç denetim organizasyon şemasında üçüncü hatta hem yönetim fonksiyonundan hem de diğer fonksiyonlardan bağımsız şekilde konumlanır. Üç hatlı savunma süreci, fonksiyonlar arasında işbirliği ve koordinasyonla işletmenin maruz kaldığı tüm risklere karşı işletmeyi koruma kalkanlarıyla çevreler. Diğer taraftan, risklerle çevrili sürekli değişen işletme çevresi ve sayıları giderek artan gönüllü ve zorunlu sınırlar, YRU faaliyetleri için birçok örgütsel modelde dördüncü savunma hattı olarak tanımlanan düzenleyici kurumlar ve bağımsız denetim ile koordinasyonun sınırlarının belirlenmesini gerekli kılmıştır.

İç denetim fonksiyonunun YRU yaklaşımına ilişkin sorumlulukları üstlenirken bağımsızlığına ve objektifliğine zarar verebilme potansiyeli olan faaliyetleri yerine getirmemesi gerekmektedir. Araştırmamız kapsamında elde edilen veriler üzerinde, iç denetçilerin üstlenmemeleri gereken sorumlulukları olarak isimlendirilen bir faktör keşfedilmiştir. Söz konusu faktörde gruplanan ifadelere iç denetçilerin verdikleri yanıtların ortalamasının 2,14 ve diğer katılımcıların yanıtlarının ortalamasının 2,15 olduğu belirlenmiştir. Söz konusu bulgular, araştırma örneklemimizin iç denetim fonksiyonunun bağımsızlığını ve objektifliğini koruması gerektiğini vurgular niteliktedir. Araştırma örnekleminin görüşlerine göre, iç denetim fonksiyonu mesleğin bağımsızlığına zarar verme potansiyeli olan görevleri yerine getirmemelidir.

Araştırmanın teorik kısmında YRU yaklaşımı, iç denetim perspektifinden tartışılmıştır. İşletmelerin güvence faaliyetlerine, risk ve kontrol fonksiyonlarına birçok fayda sunmayı vadeden YRU yaklaşımına ilişkin teorik değerlendirmeler, mevcut iç denetim literatürü, iç denetimin arka planındaki kuram, iç denetim standartları ve IIA pozisyon raporları gibi yayınları açısından tartışılmıştır. IIA, kurulduğu 1941 yılından bu yana işletme ihtiyaçları doğrultusunda iç denetimin tanımını, standartlarını veya pozisyon raporlarını güncellemektedir. IIA'yı söz konusu çalışmalarında yönlendirmek, çalışmamızın önemli gördüğümüz amaçlarından birisidir. Günümüzün küreselleşme sonucunda ulusal ve uluslararası düzenlemelerle sarılı hale gelen ekonomik düzeni, uygunluğu işletme faaliyetlerini yoğun şekilde etkileyen öne çıkarılması gereken bir kavram haline getirmiştir. Diğer taraftan, YRU yaklaşımının risk ve kontrol faaliyetlerine getirdiği felsefe, IIA'nın özellikle pozisyon raporlarında hâlihazırda kendisine yer bulmaya başlamıştır. IIA, Mesleki Uygulama Çerçevesini uygunluk gibi öne çıkan güncel işletme ihtiyaçlarına ve YRU yaklaşımı gibi yeni yönetim yaklaşımlarına göre düzenleyerek yeniden yayımlamalıdır.

### 6.2. Araştırma Sonuçları ve Öneriler

İş dünyasında yaşanan hızlı değişim, iç denetim mesleğinin kapsamına ve sorumluluklarına yön vermiştir. Artık iç denetçiler mesleğin ilk yıllarında üstlendikleri ve zamanlarının çoğunu ayırdıkları faaliyetlere çok az veya hiç zaman ayırmamaktadırlar. Günümüz işletmelerinin faaliyetlerinde etkinliği ve verimliliği artıran yaklaşımların geliştirilmesi ve çoğu zaman teknolojik çözümlerle desteklenmesi, değişen işletme faaliyetleriyle beraber iç denetçilerin yeni ve birincil sorumlulukları haline gelmiştir. Çalışmamızda işletmenin strateji, süreçler, teknoloji ve çalışanlarının düzenlenmesiyle işletme çapında yönetişim, risk yönetimi ve uygunluğu sağlamayı amaçlayan Yönetişim-Risk-Uygunluk (YRU) Yaklaşımı kapsamında iç denetimin güncel sorumlulukları değerlendirilmiştir.

İç denetim mesleği, günümüz iş dünyasında üst yöneticilerin ve yönetim kurullarının stratejik akıl ortağı haline gelmiştir. İç denetçiler, faaliyetlerin geliştirilmesi ve performansın artırılması gibi işletme amaçlarına ulaşılmasında işletme yönetiminin en başta gelen yardımcılarıdır. İç denetim, yönetişimin dört temel köşe taşından biri olarak kabul görmeye başlamıştır. İşletme çevresinin giderek daha fazla karmaşıklaşması, baş döndürücü değişimin hızı ve küreselleşme sonucu ortaya çıkan yeni risk faktörleri bir

işletme standardı haline gelen kurumsal risk yönetiminde, yönetişimin temel taşlarından biri olan iç denetime üst yönetimin desteklenmesi konusunda önemli sorumluluklar yüklemektedir. Diğer taraftan yine küreselleşme ile hız kazanan yerel ve ulusal düzenlemelerin sayısındaki artış ve işletme politikalarının ve yordamlarının bir iç düzenleme olarak görüldüğü yeni anlayış, iç denetçilerin mesailerinin önemli bir bölümünü uygunluk faaliyetleri üzerine yoğunlaştırmalarını gerekli kılmıştır. İç denetçiler artık YRU kısaltmasıyla ifade edilen bu üç kavrama odaklanmalı ve işletmelerinin amaçlarına ulaşması için katma değer yaratan çözümleri anlamaya çalışmalıdır.

YRU kısaltması, YRU bileşenleri olarak ifade edilen bu üç kavramın birlikte ele alınması gerektiğini savunan ve işletmenin örgüt yapısı, organizasyon şeması ve organizasyon el kitabının bu anlayışla düzenlenmesi gerektiğini savunan bir yaklaşıma evrilmiştir. Bu yaklaşım, işletmenin risk ve kontrol fonksiyonlarının birlikte çalışmasını kolaylaştıran bütünleşik bir anlayışla işbirliği ve eşgüdüm içinde çalışması gerektiğini savunur. YRU yaklaşımının arka planında, işletmenin çalışanlarının, stratejilerinin, süreçlerinin ve teknolojilerinin düzenlenmesi ile işletme fonksiyonlarının ortak taksonomi, dil ve bilgi mimarisini elde edebilmesi yer alır. Endüstri 4.0 çağını yaşadığımız günümüz işletme çevresinde, YRU yaklaşımının uygulanabilmesi, YRU yaklaşımının savunduğu felsefeye hizmet edebilecek teknoloji altyapısına bağlıdır. Birçok teknoloji sağlayıcısının sunduğu YRU yazılımları, işletmelerin imdadına yetişmiştir.

Son yıllarda gelişen yeni yönetim yaklaşımları ve teknolojik ilerlemeler konusunda işletme içinde öncü olması beklenen iç denetim fonksiyonu, işletmenin teknoloji altyapısının YRU yaklaşımına uygun şekilde düzenlenmesi sürecinde, YRU yazılım sağlayıcısının seçiminden hangi birimlerin ya da çalışanların hangi düzeyde yetkilendirilmesine gerektiğine kadar birçok konuda danışmanlık faaliyetleriyle üst yönetimin yanında olmalıdır. İç denetim fonksiyonundan YRU yaklaşımının bir işletmede benimsenmesi sürecinde, danışmanlık ve güvence rolünün ötesinde Üç Hatlı Savunma Modeli çerçevesinin sınırlarını aşmadan katılımcı rolünü de üstlenmesi beklenmektedir. OCEG Yetenek Modeli 3.0, diğer işletme fonksiyonları ile beraber YRU süreçlerinin merkezine oturttuğu iç denetim fonksiyonuna söz konusu rolü üstlenme noktasında kapsamlı bir rehber niteliğindedir.

Tez çalışmamız, tümdengelim akıl yürütme metodolojisine uygun olarak kurgulanmıştır. Çalışma kapsamında ele alınması gereken kavramlar, tümelden tikele doğru ele alınmış ve kavramlar arasındaki ilişkiler araştırma bölümünde analiz edilmiştir. Çalışmamızın teorik bölümünde, iç denetim tarihsel gelişimi çerçevesinde denetim kuramıyla ilişkilendirilerek, güncel bakış açısını yansıtacak şekilde ele alınmıştır. İşletmelerin çalışanları, stratejileri, teknolojileri ve süreçleri üzerinde yarattığı dönüşüm sonucunda sayısız faydalar getirdiği savunulan YRU yaklaşımı, iç denetçilerin bu yaklaşımın neresinde olacağı üzerinde tartışılarak incelenmiştir. Son 20 yılda işletme çevresinin yaşadığı dönüşüm sonucunda, günümüz iç denetçilerinin yoğun mesai harcadıkları kavramlar olan YRU bileşenleri, araştırma modeli ile tutarlı olarak, iç denetçilerin sorumlulukları açısından değerlendirilmiştir. Son bölümde literatür ve uzman görüşleri değerlendirilerek oluşturulan veri toplama aracı ile elde edilen veriler üzerinde, iç denetimin sorumlulukları ile YRU yaklaşımı arasında var olması beklenen ilişkiler, kurgulanan araştırma modeli ile test edilmiştir.

İç denetim sorumluluklarının YRU yaklaşımının faydaları üzerindeki etkisini inceleyen araştırma modeli, madde havuzu değerlendirme süreciyle oluşturulan veri toplama aracı ile TİDE üyesi iç denetçilerden elde edilen veriler üzerinde test edilmiştir. Öncelikle AFA ile veri seti içindeki yapılar ortaya çıkarılmış, literatür ve uzman görüşleri doğrultusunda isimlendirilmiştir. İç denetimin sorumlulukları ve YRU yaklaşımının faydalarına yönelik olarak ölçüm modelleri oluşturulmuş ve DFA ile doğrulanmıştır. İç denetimin sorumlulukları; yönetişim, risk yönetimi, uygunluk, teknoloji ve üstlenilmemesi gereken risk yönetimi sorumlulukları olmak üzere beş boyutta, YRU yaklaşımının faydaları tek boyutta açıklanmıştır. Son aşamada, yapısal model oluşturulmuş ve öngörülen modelde yer alan hipotezler test edilmiştir.

Modelin analizi sonucunda, iç denetimin sorumluluklarına yönelik faktörlerden uygunluk sorumlulukları faktöründeki değişimi, en çok U8 (İşletme faaliyetleri ile ilgili düzenli olarak uygunluk risk değerlendirmesi yapar) (%82) ve en az (%74) U10 (Hem ulusal hem uluslararası güncel düzenlemelerin takip edilmesini kolaylaştıran kontrol yordamları geliştirir) açıklamıştır. Bilgi teknolojileri faktöründeki değişimi, en çok BT9 (İşletmede sürekli denetim için otomatik kontrol modellerinin uygulanmasına destek olur) (%83) ve en az BT2 (YRU yazılımlarının tasarımını ve işleyişini düzenli olarak gözden geçirir) (%72) açıklamıştır. Risk yönetimi faktöründeki değişimi, en çok R11 (İkinci savunma hattında bulunan risk ve kontrol birimlerinin etkinliğini geliştirir) (%82)

ve en az R2 (Temel risklerin üst yönetim tarafından yönetilip yönetilmediğini inceler) (%67) açıklamıştır. Yönetişim faktöründeki değişimi, en çok Y9 (YRU yaklaşımını desteklemek amacıyla iç kontrol, risk yönetimi, yönetişim, sürdürülebilirlik gibi konularda çerçeve ve rehberleri bilir) (%82) ve en az Y4 (İşletmede yönetişimi geliştirecek politika, yordam ve süreçlerin geliştirilmesine destek olur) (%69) açıklamıştır. Üstlenilmemesi gereken risk yönetimi faktöründe değişimi, en çok R9 (Üst yönetimin risk yönetimi çalışmalarında etkinliğini garanti eder) (%82) ve en az R13 (Risklere karşı uygulanacak eylemleri yönetim adına uygular) (%72) açıklamıştır. YRU yaklaşımının faydaları faktöründe ise, değişim en çok YRU11 (Stratejik planlamanın risk bilinciyle oluşturulmasını sağlar) (%89) ve en az YRU6 (Risk yönetimini işletmeye değer katan bir faaliyete dönüştürür) (%74) maddesinde açıklanmaktadır. Yapısal modelin analizi sonucunda yönetişim, bilgi teknolojileri ve risk yönetimi sorumlulukları faktörleri ile YRU yaklaşımının faydaları arasında pozitif yönlü üstlenilmemesi gereken risk yönetimi sorumlulukları ile YRU yaklaşımının faydaları arasında negatif yönlü istatistiksel olarak anlamlı ilişkiler olduğu anlaşılmıştır. Uygunluk sorumlulukları ile YRU yaklaşımının faydaları arasında ise 0.05 anlamlılık düzeyinde ilişki yoktur. Dolayısıyla $H_2$-$H_3$-$H_4$ ve $H_5$ hipotezleri kabul edilmiş, $H_1$ hipotezi reddedilmiştir. Yapısal modelin sonuçları, iç denetimin bilgi teknolojileri, risk ve yönetişim sorumluluklarındaki 1 birimlik artışın YRU yaklaşımının faydaları üzerinde sırasıyla 0.18, 0.33 ve 0.20 birimlik bir artışa neden olacağını ifade etmektedir. İç denetimin üstlenmemesi gereken risk sorumluluklarındaki 1 birimlik azalış ise, YRU yaklaşımının faydaları üzerinde 0,20 birimlik artışa neden olur.

Araştırma kapsamında geliştirilen diğer hipotezleri test etmek amacıyla, veri toplama aracı ile TİDE üyesi iç denetçilerle birlikte KGK'dan yetki belgesi almış ve fiili olarak mesleği icra eden bağımsız denetçilerden ve Borsa İstanbul'da hisseleri işlem gören şirketlerin yöneticilerinden veri toplanmıştır. Veri toplama aracı ile toplanan veriler üzerinde, iç denetçilerin sorumlulukları ve YRU yaklaşımının faydalarına yönelik iki örneklem grubunun olması gereken duruma ve uygulamaya yönelik görüşlerini karşılaştırmak amacıyla parametrik testler yürütülmüştür.

Yapılan analizlerin sonuçlarına göre iç denetçilerin sorumluluklarına ilişkin olması gereken duruma ve uygulamadaki duruma ilişkin görüşlerinde sadece bilgi teknolojileri sorumluluklarında olması gereken durum lehine anlamlı bir farklılık belirlenmiştir. Aynı analizin bağımsız denetçiler ve işletme yöneticilerinden oluşan diğer grubun görüşleri

üzerinde yürütülmesi sonucunda, üstlenilmemesi gereken risk sorumlulukları dışında tüm sorumluluklar arasında anlamlı olması gereken durum lehine farklılık tespit edilmiştir. Elde edilen bulgular, iç denetim hizmetlerini gözlemleme şansı bulunduğu varsayılan örneklem grubunun, iç denetçilerin daha fazla sorumluluk üstlenmesi gerektiği ya da uygulamada sorumluluklarını gerektiği gibi üstlenmedikleri görüşlerinden birine sahip oldukları şeklinde yorumlanabilir. Görüşler birlikte değerlendirildiğinde, iç denetçilerin bilgi teknolojileri sorumlulukları konusunda eksikliklerini kabul ettikleri ya da daha fazla sorumluluk üstlenmek için çaba göstermeleri gerektiği görüşüne sahip oldukları anlaşılır. Her iki yorum da, iç denetim mesleği için teknolojinin karşı konulamaz ya da yok sayılamaz hale geldiğini gösterir. Diğer taraftan her iki örneklem grubunun üstlenilmemesi gereken risk yönetimi sorumlulukları konusunda, iç denetçilerin Mesleki Uygulama Çerçevesi ve IIA'nın pozisyon raporlarında iç denetçilerin bağımsızlığını korumak amacıyla getirdiği düzenlemelere mutlak şekilde uygun davrandığı görüşünde oldukları anlaşılmıştır.

İç denetçilerden oluşan örneklem grubu ile bağımsız denetçiler ve işletme yöneticilerinden oluşan örneklem grubunun hem olması gereken duruma hem de uygulamaya yönelik görüşleri ayrı ayrı analiz edilmiştir. Olması gereken duruma yönelik görüşler açısından iki grubun ortalamaları arasında iki faktörde istatistiksel olarak anlamlı farklılık tespit edilmiştir. Diğer katılımcılardan oluşan grubun uygunluk ve yönetişim sorumluluklarına ilişkin görüşleri, iç denetçilerin görüşlerinden anlamlı şekilde yüksektir. Diğer katılımcılar, iç denetimin uygunluk ve yönetişim konusunda daha fazla sorumluluk üstlenmesi gerektiği görüşündedirler. Öte yandan, uygulamaya yönelik görüşler arasında, üstlenilmemesi gereken risk yönetimi sorumlulukları dışında tüm iç denetim sorumluluklarında iç denetçiler lehine istatistiksel olarak anlamlı farklılık tespit edilmiştir. İç denetçilerin görüşleriyle karşılaştırıldığında diğer katılımcılardan oluşan grup, iç denetçilerin uygulamada daha az sorumluluk üstlendiği görüşündedirler.

Son olarak iki örneklem grubunun YRU yaklaşımının faydalarına yönelik görüşleri karşılaştırılmıştır. Yapılan analizlerin sonuçları, iç denetçilerin görüşlerinin diğer katılımcıların görüşlerinden istatistiksel olarak yüksek olduğunu göstermiştir. İç denetçilerin diğer katılımcılara göre, YRU yaklaşımının faydalarına yönelik görüşlerinin genel olarak daha olumlu olduğu anlaşılmıştır. Bu sonuç, YRU yaklaşımının tüm işletme çalışanlarının işlerini kolaylaştırmakla beraber, daha çok risk ve kontrol çalışanlarının iş süreçlerini geliştirmesi, özellikle de güvence çalışanlarının ortak paylaşılan güvence

evreni üzerinde işbirliği ve eşgüdüm içinde çalışabilmesini sağlaması gibi iç denetim fonksiyonuna fayda sağlamaya yönelik spesifik özelliklere sahip olmasıyla ilişkilendirilebilir.

YRU yaklaşımının getirdiği bütüncül bakış açısı ve işbirliği kültüründen en fazla fayda sağlayan tarafların başında güvence çalışanları gelmektedir. YRU yaklaşımının sağladığı ortak süreçler, terminoloji, organizasyonel ve teknolojik altyapı ve bütüncül bakış açısı üzerinde düşünüldüğünde, işletme içinde YRU yaklaşımından en fazla fayda sağlayan taraflar (1) İç denetçiler, (2) İkinci savunma hattında konumlanan risk ve kontrol fonksiyonları ve (3) Üst yönetim ve yönetim kurulu olarak üçe ayrılabilir. Araştırmamız kapsamında iç denetçilerin likert ölçeğiyle kurgulanan YRU yaklaşımının faydalarına ilişkin sorulara verdikleri yanıtların ortalamaları 4,37 olmuştur. Bağımsız denetçilerden ve işletme yöneticilerinden oluşan diğer katılımcıların yanıtlarının ortalamaları 4,20 olmuştur. Söz konusu bulgular, araştırma örneklemimizin YRU Yaklaşımının faydaları hakkındaki önermeleri doğruladığını göstermiştir. Ayrıca yapısal model, iç denetim fonksiyonunun sorumluluklarının YRU yaklaşımının faydalarını pozitif yönde, üstlenmemesi gereken sorumluluklarının ise negatif yönde etkilediğini göstermiştir. Çalışmamız kapsamında ayrıntılı olarak ele aldığımız YRU yaklaşımının, işletmelere sağladığı önemli faydalar kısaca şöyle özetlenebilir:

- Riskler, kontroller, kanunlar, yönetmelikler, politikalar ve denetim sonuçlarının risk ve uygunluk yöneticileri ve çalışanları, iç denetçiler ve işletme üst yönetimi arasındaki işbirliğini kolaylaştıran ortak bir çerçevede ele alınmasını sağlar. Böylece en iyi çözümlerin geliştirilmesi ve uygulanmasını kolaylaştırır.
- İşletmede potansiyel risklerin, uygunluk yükümlülüklerinin ve yönetişim sorunlarının kapsamlı bir bakış açısıyla kontrol altında tutulmasını sağlar. YRU bileşenleri arasındaki bağlantıların ortaya çıkarılması ile stratejik amaçların ve iş süreçlerinin daha proaktif olarak izlenmesi sağlanır.
- Stratejileri, iş süreçlerini ve işletme amaçlarını tehdit eden risklerin ve ilgili sorunların tutarlı risk bilgisiyle daha proaktif şekilde yönetilmesini sağlar ve potansiyel olumsuzlukların tespit edilip, ortaya çıkmadan önüne geçilmesini sağlar.
- Yönetişim, risk yönetimi ve uygunluk süreçlerinin etkinliğini ve verimliliğini arttırır. Ortak süreçler, Endüstri 4.0 unsurları olarak tanımlanan ileri teknolojilerle birlikte kontrollerin ve risklerin sürekli izlenmesine mümkün hale getirir. Risk ve

uygunluk çalışanları ile iç denetçiler arasında işbirliğini geliştirerek risk değerleme gibi rutin süreçlerin daha kolay ve düşük maliyetle yönetilmesini sağlar.

- YRU yaklaşımının getirdiği bütüncül bakış açısı ile işletme faaliyetlerinin ve iş süreçlerinin merkezine tutarlı risk görünümünü ve bilgilendirilmiş stratejik karar alma süreçlerini oturtan yeni bir kurumsal risk yönetimi felsefesidir. YRU yaklaşımı, kurumsal risk yönetimini kapsar. İşletme faaliyetlerinin maruz kaldığı risk faktörlerinin izlenmesi ve yönetilmesi birincil amaçlarındandır. Başarısız kontrollerin ve kayıplara neden olan olayların işletme faaliyetlerine etkisi, veriden öğrenen ileri teknolojiler yardımıyla değerlendirilmeli ve tekrarının hatta hiç ortaya çıkmasının önüne geçilmeye çalışılmalıdır.
- Yönetişim, risk yönetimi ve uygunluk ihtiyaçlarının kontrol, denetim, risk yönetimi veya uygunluk gibi farklı fonksiyonlarda tutarlı bir şekilde ele alınması gerektiği konusundaki belirsizliği ortadan kaldırır. İşletme içinde işbirliği ve eşgüdüm içerisinde çalışılmasını, getirdiği örgütsel ve teknolojik altyapıyla destekler. İşletme fonksiyonları arasında ortak terminoloji ve taksonominin geliştirilmesini sağlar. İşletme içi ve dışı raporlama faaliyetlerinin tutarlılığını artırır. YRU yaklaşımının savunduğu ortak çalışma kültürü, finansal verilerin yanında işletme faaliyetleriyle ilgili finansal olmayan verilerin sunulduğu sürdürülebilirlik ve entegre raporların çok daha kolay hazırlanmasını sağlar.
- Uygunluk ve risk yönetimi açısından daha fazla güvence sağlanmasını destekler. Uygunluk, risk yönetimi ve denetim başarısını yükseltir. İşletme birimlerinin, yönetim kurulu ve diğer stratejik karar alıcılara uygun seviyede bilgi verdiklerinden emin olunmasına katkı sağlar.

Araştırmamızın bir başka önemli bulgusu, işletmenizde kullanılan risk yönetimi modeli nedir? Sorusuna, örneklemimizde yer alan iç denetçiler ve işletme yöneticilerinin en fazla COSO KRY ve ISO31000 cevabını vermiş olmasıdır. Yeni KRY çerçeveleri, etkin risk yönetiminin, işletmenin iç kontrolün YRU yaklaşımının savunduğu bütünleşik yapıya uygun olarak tasarlanması ile mümkün olacağını savunmaktadır. Araştırma örneklemimizde elde ettiğimiz bu bulgu, daha önce yapılan Türkçe ve Yabancı çalışmaları desteklemiştir. Yine bu soruya verilen az sayıdaki (12, %4) YRU yanıtı, yabancı çalışmalara yakın bir oranda gerçekleşmiştir. Bu durum, risk yönetimi faaliyetlerine bütüncül bir bakış açısı sunan yeni bir yönetişim yaklaşımı olan YRU

açısından, Türkiye'de mesleği icra eden iç denetçilerin Dünya'yı yakından takip ettiği şeklinde değerlendirilebilir.

Çalışmamızın sonuçları, gelecekte yapılacak çalışmalara ilham verme potansiyeline sahiptir. Ayrıca elde edilen sonuçlar doğrultusunda yapılacak çalışmalara yönelik öneriler getirebilmek mümkündür. Araştırmada oluşturduğumuz veri toplama aracı, gelecekte yapılacak çalışmalarda, araştırma desenine uyarlanarak ve geliştirilerek kullanılabilir. Diğer taraftan araştırma modeli, farklı veri toplama ve analiz yöntemleriyle kurgulanabilir. Böylece araştırma sonuçları, gelecekte yapılan çalışmalarla sınanmış olacaktır. İç denetim sorumlulukları ile YRU yaklaşımı ilişkisi, bizim araştırma modelimizden farklı olarak dolaylı etkileri keşfetmeyi amaçlayan araştırma modelleriyle daha ayrıntılı olarak değerlendirilebilir. Araştırmamız kapsamında katılımcıların değerlendirmeye alınmayan yaş, cinsiyet ve mesleki tecrübe gibi demografik özellikleri gelecekte yapılacak araştırmaların kapsamına alınabilir. Araştırmamız Türkiye'de mesleğini icra eden katılımcılardan oluşan örneklem üzerinde uygulanmıştır. Farklı ülkelerdeki örneklemler üzerinde yürütülen çalışmalar, farklı özelliklere sahip ülkelerle durumun karşılaştırılabilmesini sağlayacaktır.

## KAYNAKÇA


Abdioğlu, Hasan (2007). *İşletmelerde Kurumsal Yönetim Anlayışı Kapsamında İç Denetimin Rolü ve İMKB-100 Örneği*. Yayımlanmamış Doktora Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Muhasebe Finansman Bilim Dalı.

Abu-Musa, A. A. (2008). Information technology and its implications for internal auditing: An empirical study of Saudi organizations. *Managerial Auditing Journal*, 23(5), 438-466.

Acar, İ. A. (2008). İç Denetim -Stratejik Plan- Performans Yönetimi Çerçevesinde Kavramsal Değerlendirmeler. *Yerel Siyaset Dergisi*, 26, 79-83.

Adams, M. B. (1994). Agency theory and the internal audit. *Managerial Auditing Journal*, 9(8), 8-12.

Adams, P., Cutler, S., McCuaig, B., Rai, S. & Roth, J. (2016). *Sawyer's İç Denetçiler için Rehber* (Cilt 3) (Çev: Çetin Özbek). İstanbul: Türkiye İç Denetçiler Enstitüsü Yayınları, Yayın No: 10.

AICPA, (1991). *American Institute of Certified Public Accountants, Statement on Auditing Standards* (SAS) No.65: The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statement.

Akarkarasu, N. (2000). *Halka Açık Şirketlerde İç Denetim ve Denetim Kurullarının Etkinleştirilmesi İçin Öneriler* (Yeterlilik Etüdü). İstanbul: Sermaye Piyasası Kurulu Denetleme Dairesi.

Akbulut, Y. (2010). *Sosyal bilimlerde SPSS uygulamaları: Sık kullanılan istatiksel analizler ve açıklamalı SPSS çözümleri*. İdeal Kültür Yayıncılık.

Aksu, G., Eser, M. T., & Güzeller, C. O. (2017). *Açımlayıcı ve doğrulayıcı faktör analizi ile yapısal eşitlik modeli uygulamaları*. Ankara: Detay Yayıncılık.

Aktan, C. C. (2006). *Kurumsal Şirket Yönetimi*. Ankara: SPK Yayınları.

Alparslan, M. (2000). Bankalarda Kurumsal Yönetim. *Bankacılar Dergisi*, 32, 94-101.

Alptürk, E. (2008). *Finans, Muhasebe ve Vergi Boyutlarında İç Denetim Rehberi*. Ankara: Maliye ve Hukuk Yayınları.

Anand, S. (2010). Technology and the Integration of Governance, Risk Management and Compliance. *Financial Executive*. 26 (10), Aralık, 57-58.

Anderson, D. J. & Eubanks, G. (2015). *Leveraging Coso Across The Three Lines of Defense*. Florida: International Internal Auditors (IIA).

Arens, A., Elder, R. J. & Beasley, M. (2012). *Auditing and Assurance Services: an Integrated Approaches*. New Jersey: Pearson Prentice Hall.

Arı, E. & Yılmaz, V. (2015). Banka Hizmet Kalitesi Boyutları İle Banka Sadadakati Arasındaki İlişkilerin Servqual Ve Yapısal Eşitlik Modeli İle İncelenmesi: İİBF

Öğrencileri Üzerine Bir Uygulama. *Suleyman Demirel University Journal of Faculty of Economics & Administrative Sciences*, 20 (3), 121-135.

Arın, T., Kesmez, N., & Gören, İ. (2000). *Parlamento ve Sayıştay Denetimi*. İstanbul: Türkiye Ekonomik ve Sosyal Etüdler Vakfı.

Ashbaugh, H. & Warfield, T. D. (2003). Audits as a corporate governance mechanism: evidence from the German market. *Journal of International Accounting Research*, 2, 1-21.

Atamer, M. (2006). *Halka Açık Anonim Şirketlerde Kurumsal Yönetim ve Doğrudan Yabancı Yatırımlar Açısından Değerlendirilmesi* (Uzmanlık Tezi). Ankara: Hazine Müsteşarlığı.

Aydemir, Birol (2005). Stratejik Yönetim ve Bütçe. *Türkiye'de Yeniden Mali Yapılanma:20. Maliye Sempozyumu* (23-27 Mayıs), Denizli: Pamukkale Üniversitesi İİBF, Yayın No: 1, s.24-33.

Aysan, M. (2007). *Kurumsal Yönetim ve Risk*. İstanbul: Elit Ofset Matbaacılık.

Bace, J., Rozwell, C., Feiman, J. & Kirwin, B. (2006). *Understanding the Costs of Compliance*. Stamford: Gartner Research, ID Number: G00138098, 1-19.

Bagozzi, P. R. (1981).Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. A Comment. *Journal of Marketing Research*, 18 (3), 375-381.

Bağcı, B. (2014). Bilgi Teknolojileri Standartları ve Çerçeveleri. H. Kıral (Ed.), *İç Denetim Yönetime Değer Katmak* içinde (s. 343-374). Ankara: İç Denetim Koordinasyon Kurulu.

Banham, R. (2007). Is ERM GRC or Vice Versa? *Treasury & Risk*, June, 48-50.

Bayram, N. (2010). *Yapısal eşitlik modellemesine giriş amos uygulamaları*. Bursa: Ezgi Kitabevi.

Blunch, N. (2012). *Introduction to structural equation modeling using IBM SPSS statistics and AMOS*. Los Angeles: Sage.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Lapides, P. D. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting Horizons*, 14(4), 441-454.

Beasley, M. S., Clune, R. & Hermanson, D. R. (2005). ERM: A Status Report. *Internal Auditors*, February, 62 (1), 67-73.

Beasley, M. S., Clune, R., & Hermanson, D. (2006). *The impact of enterprise risk management on the internal audit function*. Kennesaw, GA: Kennesaw State University.

Beasley, M. S., Frigo, M.L. & Litman, J. (2007). Strategic Risk Management: Creating and Protecting Value. *Strategic Finance*. Mayıs, 88 (11), 24-53.

Benson, J. (2007). The Importance of Monitoring. *The Internal Auditor*, 64 (4), August, 85-89.

Berle, A., & Means, G. (1932). *Private property and the modern corporation*. New York: Mac-millan.

Blokdijk, J. H., Drieënhauizen, F. & Wallage, P. (1995). *Reflections on Auditing Theory, A Contribution from the Netherlands*. Amsterdam: Kluwer/Limperg Instituut-Reeks.

Bierstaker, J., L., Burnaby, P. & Thibodeau, J. (2001). The impact of information technology on the audit process: an assessment of the state of the art and implications for the future. *Managerial Auditing Journal*, 16 (3), 159-164.

Bonazzi, R., Hussami, L. & Pigneur, Y. (2009). Compliance management is becoming a major issue in IS design. A. D'Atri & D. Saccà (Eds.), *Information systems: People, organizations, institutions, and Technologies* içinde Berlin: Physica-Verlag HD, 391-398.

Boone, L. E. & Kurtz, D. L. (2013). *Contemporary Business*. Chicago: Dryden Press.

Bozkurt, C. (2010). Risk, Kurumsal Risk Yönetimi ve İç Denetim. *Kamu İç Denetçileri Derneği Denetişim Dergisi*, 4, 17-30.

Broady, V. D., & Roland, H. A. (2008). *SAP GRC for dummies*. Hoboken, New Jersey: Wiley.

Brown, R. G. (1962). Chancing Audit Objectives and Techniques. *The Accounting Review*, 37 (4), 696-703.

Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of Big Data's impact on audit judgment and decision making and future research directions. *Accounting Horizons*, 29(2), 451-468.

Burns, P. & Nordstrom, P. (2015). *Compliance & Internal Audit Collaboration Developing a compliance third line of defense*. London: PricewaterhouseCoopers.

Byrne, B. M. (2011). *Structural equation modeling with AMOS Basic concepts, applications, and programming* (Multivariate Applications Series), New York: Routledge.

Cadbury, A. (1992). *Report of The Committee on The Financial Aspects of Corporate Governance (Cadbury Report)*. London: Gee Professional Publishing.

Cangemi, M. P. (2015). Staying a Step Ahead: Internal Audit's Use of Technology. Altamonte Springs, Florida: IIA Research Foundation.

Cangemi, M. P. (2016). Views on internal audit, internal controls, and internal audit's use of technology. *EDPACS*, 53(1), 1-9.

Carcello, J. V., Hermanson, D. R., & Ye, Z. (2011). Corporate governance research in accounting and auditing: Insights, practice implications, and future research directions. *Auditing: A Journal of Practice & Theory*, 30(3), 1-31.

Carcello, J., V., & Neal, T., L. (2000). Audit Committee Composition and Auditor Reporting. *The Accounting Review*, 75, (October), 453-467.

Castanheira, N., Rodrigues, L.L. and Craig, R. (2010). Factors associated with the adoption of risk- based internal auditing. *Managerial Auditing Journal*, Vol. 25 No. 1, 79- 98.

Cau, D. (2014). Governance risk and compliance (GRC) software business needs and market trends. *Deloitte*.

Cemalcılar, Ö. ve Önce, S. (1999). *Muhasebenin Kuramsal Yapısı*. Anadolu Üniversitesi Yayın No:1093, Eskişehir: T.C. Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Yayınları.

Cendrowski, H., & Mair, W. C. (2009). *Enterprise risk management and COSO: a guide for directors, executives and practitioners*. Newyork: John Wiley & Sons.

Cengiz, S. (2013). İşletmelerde Kurumsal Yönetim Kapsamında İç Denetimin Yeri ve Önemi: Borsa İstanbul'da Bir Araştırma. *Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 15(2), 403-448.

Chambers, A., D. (2014). The Current State of Internal Auditing: A Personal Perspective and Assessment. *EDPACS The EDP Audit, Control, and Security Newsletter*, 49 (1), 1-14.

Chapman C. & Anderson U. (2002). *Implementing the Professional Practices Framework*. Florida: The Institute of Internal Auditors.

Chorafas, D. N. (2001). *Implementing and auditing the internal control system*. Newyork: Palgrave Macmillan.

Christopher, J. (2015). Internal audit: Does it enhance governance in the Australian public university sector?. *Educational Management Administration & Leadership*, 43(6), 954-971.

Chukwunedu, O., S. & Okoye, E., I. (2011). *Forensic Accounting and Audit Expectation Gap - The Perception of Accounting Academics*. Working Paper Series.

Clendenen, P. (2007). My biggest concern is that ERM will devolve to focus exclusively on regulatory compliance and governance. *Treasury & Risk*, June, 50-51.

Coderre, D. G. (2009). *Internal audit: efficiency through automation*. New Jersey: John Wiley & Sons.

Cohen, J. (1988). Statistical Power Analysis For The Behavioral Sciences (2nd.). Hillsdale, NJ: Erlbaum.

Cohen, D. A., Dey, A. & Lys, T. Z. (2008). Real and Accrual Based Earnings Management in the Pre- and Post- Sarbanes- Oxley Periods. *The Accounting Review*, 83 (3), ss.757-787.

Cohen, J., Krishnamoorthy, G., & Wright, A. M. (2002). Corporate governance and the audit process. *Contemporary accounting research*, 19(4), 573-594.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise Risk Management Framework (Draft),* Amerika: COSO.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control - Integrated Framework Executive Summary*. North Carolina: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2016). *Enterprise Risk Management Aligning with Strategy and Performance*. Amerika: COSO.

Cömert, N. (2016). İşletmelerde kontrol ve denetim kavramlarının doğru kullanılması amacına yönelik kavramsal bir inceleme. *Marmara Business Review*, 1 (1), June, 1-20.

Çelik, H. E., & Yılmaz, V. (2013). *Yapısal eşitlik modellemesi temel kavramlar-uygulamalar-programlama*. Ankara: Anı Yayıncılık.

Delmar, Y., Harper, T., Cooney, J. & Switzer, C. (2016). *How Should the Chief Audit Executive Be Talking About GRC?* Scottsdale, Arizona: OCEG.

Deloitte (2006). *Nedir Bu Kurumsal Yönetim?* Kurumsal Yönetim Serisi, Türkiye Kurumsal Yönetim Derneği ve Deloitte Ortak Yayını, İstanbul: Deloitte.

Deloitte (2008). *Kurumsal Yönetim İlkeleri Bağlamında Genel Kurulun ve Yönetim Kurulunun Karşılıklı Konumu*. Kurumsal Yönetim Serisi, Türkiye Kurumsal Yönetim Derneği ve Deloitte Ortak Yayını, İstanbul: Deloitte.

DeVellis, R. F. (2003). Scale development: Theory and applications (Vol. 26) (Second Edition). United States of America, California: Sage publications.

Dima, F. C. (2013). Risk Management From The Perspective of Internal Audit. *Management Strategies Journal*, 22, 105-110.

Dinç, E. & Abdioğlu, H. (2009). İşletmelerde Kurumsal Yönetim Anlayışı ve Muhasebe Bilgi Sistemi İlişkisi: İMKB-100 Şirketleri Üzerine Ampirik Bir Araştırma. *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 12 (21), ss.157-184.

Dittmar, L. & B. Kobel. (2008). The Risk Intelligent CIO. *Risk Management* (Mart): 42.

Doğan, M. (2007). *Kurumsal Yönetim*. Ankara: Siyasal Yayınevi.

Ducu, C. M. (2013). Importance of Internal Audit within An Entity. *Management Strategies Journal*, 22 (Special), 111-116.

Duits, H. B. (2012). *The added value of auditing in a non-mandatory environment*. Amsterdam: Vossiuspers UvA - Amsterdam University Press.

Dupuis, M., Endicott-Popovsky, B., Wang, H., Subramaniam, I. & Du, Y. (2011). Top-Down Mandates and the Need for Organizational Governance, Risk Management, and Compliance in China: A Discussion. *China-USA Business Review*, 10 (5), 319-336.

Dündar, S., Candemir, Ö., Demiray, E., Genç Kumtepe, E., Öztürk, S., Sağlık Terlemez, M., Ulutak, İ. (2017). Anadolu Üniversitesi çalışanlarının açık ve uzaktan öğretime ilişkin tutumları. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 3 (4), 187-227.

Eggert, M. (2014). *Compliance Management in Financial Industries*. Berlin: Springer International Publishing.

Eisenhardt, K. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review*, 14 (1), 57-74.

Elbannan, M. A. (2009). Quality of internal control over financial reporting, corporate governance and credit ratings. *International Journal of Disclosure and Governance*, 6(2), 127-149.

Erdoğan, M. (2012). İç Denetim. M. Erdoğan (Ed.) *Denetim* içinde (s. 104-141). Eskişehir: Anadolu Üniversitesi, Açıköğretim Fakültesi Yayınları.

Erdoğan, M. (2005). *Denetim*. Ankara: Maliye ve Hukuk

Erdoğan, M. (2017). Denetim 4.0 ve Ötesi. *XII. Uluslararası Türkiye Muhasebe Denetimi Sempozyumu*'unda sunulan bildiri (6-10 Aralık 2017), Antalya:Regnum Carya Hotel.

Erdoğan, M. (2017). Sıfırıncı Yasa. *Muhasebe Bilim Dünyası Dergisi*, 19 (3), 746-759.

Erdönmez, A. P. (2003). Türkiye'de 2001 Yılındaki Mali Kriz Sonrasında Kurumsal Sektörde Yeniden Yapılandırma. *Bankacılar Dergisi*, 47, 38-55.

Eroğlu, C. A. (2003). *Kurumsal Yönetim İlkeleri Çerçevesinde Kamunun Aydınlatılması*. SPK Yeterlilik Etüdü, Ankara: Sermaye Piyasası Kurulu.

Eşkazan, A. R. (2005). Risk Odaklı İç Denetim Planlaması. *TİDE İç Denetim*, Bahar, 32-33.

Fadzil, F. H., Haron, H. & Jantan, M. (2005). Internal auditing practices and internal control system. *Managerial Auditing Journal*, 20 (8), 844 – 866.

Fama, E. (1965). Random Walks in Stock Market Prices. *Financial Analysts Journal*, 21 (5), 55-60.

Fıkırkoca, M. (2003). *Bütünsel Risk Yönetimi*. Ankara: Pozitif Matbaacılık.

Financial Reporting Council. (2005). *Internal Control: Revised Guıdance for Directors on The Combined Code*. London: The Financial Reporting Council.

Florea, R. (2013). Internal Audit and Corporate Governance. *Economy Transdisciplinarity Cognition*, 16 (1), 79-83.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18* (1), 39-50.

Fowzia, R. (2010). Co-operation between Internal and External Auditors: A Comparative Study on Nationalized and Foreign Banks in Bangladesh. *World Journal of Management*, 2 (2), 22-35.

Fraser, I., & Henry, W. (2007). Embedding risk management: structures and approaches. *Managerial Auditing Journal*, 22(4), 392-409.

Frigo, M. L. & Anderson, R. J. (2009a). A strategic framework for governance, risk and compliance. *Strategic Finance*, 90 (8), 20-61.

Frigo, M. L. & Anderson, R. J. (2009b). Strategic GRC: 10 Steps to Implementation. *Internal Auditor*, June, 33-37.

Garsoux, M. & Soenen P. (2017). A Global approach to Risk and Control. White paper. ISACA Report.

George, D & Mallery, P. (2010). *SPSS for windows step by step: A simple study guide and reference*. 17.0 update, Boston: Pearson Education.

Ghiran, A. M. & Bresfelean, V. P. (2012). Emerging Markets Queries in Finance and Business Compliance Requirements for Dealing with Risks and Governance. *Procedia Economics and Finance*, 3, 752-756.

Gillis, A. (2013). Our Thoughts On: Internal Audit vs. Compliance. *Internal Auditor*, September, 1-5.

Goodwin, J., & Seow, J. L. (2002). The influence of corporate governance mechanisms on the quality of financial reporting and auditing: Perceptions of auditors and directors in Singapore. *Accounting & Finance*, 42(3), 195-223.

Goodwin-Stewart, J., & Kent, P. (2006). The use of internal audit by Australian companies. *Managerial Auditing Journal*, 21(1), 81-101.

Graham, L. (2015). *Internal control audit and compliance: documentation and testing under the new COSO framework*. New Jersey: John Wiley & Sons.

Gramling, A., Maletta, M., Schneider, A. & Church, B. (2004). The Role of the Internal Audit Function in Corporate Governance: A Synthesis of the Extant Internal Auditing Literature and Directions for Future Research. *Journal of Accounting Literature*, 23, 194-244.

Gramling, A. & Myers, P. (2006). Internal Auditing's Role in ERM. *Internal Auditor*, April, 52-58.

Griffiths, P. (2005). *Risk-Based Auditing*. Aldershot-England: Gower Publishing Limited.

Gupta, P., P. & Ray, M., R. (1992). The Changing Roles of the Internal Auditor. *Managerial Auditing Journal*, 7 (1), 3-9.

Güçlü, H. (2010). *Kurumsal Yönetim Uyum Derecelendirmesi*. İstanbul: İMKB Yayınları.

Güneş, F., Kızıldeniz, S., Selçuk, S., Suna, B. & Coşkun, S. (2013). Bilgi Teknolojileri Denetimi ve COBIT'in Sektörel Uygulanabilirliği. *Akademik Bilişim Konferansı*'ında sunulan bildiri. Antalya: Akdeniz Üniversitesi.

Güredin, E. (2000). *Denetim*. İstanbul: Beta.

Hair J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (2013). *Multivariate Data Analysis*. 3rd ed., New York: Pearson Education Limited.

Hahm, J., H. & Mishkin, F., S. (2000). The Korean financial crisis: an asymmetric information perspective. *Emerging Markets Review*, 1 (1), 21-52.

Hall, J. (2007). *Internal Auditing and ERM: Fitting in and Adding Value*. 2007 Esther R. Sawyer Scholarship Essay. Newyork: Instutite of Internal Auditors Research Foundation.

Hall, J. A. (2011). *Information Technology Auditing and Assurance*. Ohio: South-Western Cengage Learning.

Hardy, C. & Leonard, J. (2011). Governance, risk and compliance (GRC): Conceptual muddle and technological tangle. *ACIS 2011 Proceedings*. Australia, University of Sydney, Paper 42.

Hayes, R., Dassen, R., Schilder, A. & Wallage, P. (2005). *Principles of Auditing an Introduction to International Standards on Auditing*. London: Pearson Prentice Hall.

Hermanson, D. R., Hill, M. C., & Ivancevich, D. M. (2000). Information technology-related activities of internal auditors. *Journal of Information Systems*, 14(s-1), 39-53.

Hermanson., R., D. & Rittenberg, E., L. (2003). *Internal Audit and Organizational Governance*. Florida: Institute of Internal Auditors Research Foundation.

Herron, A. & Dholabhai, M. (2017). COSO Enterprise Risk Management Framework-Integrating Strategy and Performance. New York: PwC Governance Insights Center.

Hirth Jr, R. B. (2008). Better internal audit leads to better controls; Is your internal audit activity doing what you and your board of directors want? If not, what steps are you taking to change it? *Financial Executive*, 24 (9), 49-52.

Hopkin, P. (2010). *Fundamentals of Risk Management*. Britain, London: Kogan Page Limited.

Hu, L.T. & Bentler, P.M. (1999). Cutoff criteria for fit indexes incovariancestructure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 6, 1–55.

Huck, S. W. (2008). *Reading Statistics and Research* (5th ed.). Boston: Pearson/Allyn & Bacon.

Huibers, S. C. J. (2014). *Combining Internal Audit and Second Line of Defense Functions?* Netherlands: Institute of Internal Auditors Netherlands.

Huibers, S. C. J. (2014). *Combined Assurance: One Language, One Voice, One View*. The Global Internal Audit Common Body of Knowledge. Florida: The IIA Research Foundation.

Hutcheson, G. D., & Sofroniou, N. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models*. California: Sage.

Hutchins, G. (2018). *ISO 31000: 2018 Enterprise Risk Management*. ABD, Florida: Cerm Academy Series on Enterprise Risk Management.

IBM (2012). *Leading Through Connections: Insights From The Global Chief Executive Officer Study*. United States of America, NY: IBM Global Business Services.

Institute of Internal Auditors (IIA). (2004). *The Role of Internal Auditing in Enterprisewide Risk Management*. London: The Institute of Internal Auditors UK and Ireland.

Institute of Internal Auditors (IIA). (2010a). *Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ) Uluslararası İç Denetim Standartları*. Çeviri: Türkiye İç Denetim Enstitüsü (TİDE), İstanbul: Lebib Yalkın Yayımları.

Institute of Internal Auditors (IIA). (2010b). What GRC Could Mean to Your Organization. *Tone at the Top*, 48, Ağustos, 1-4.

Institute of Internal Auditors (IIA) (2013). *IIA Position Paper: The Three Lines Of Defense In Effective Risk Management and Control*. Florida: IIA Global.

Institute of Risk Management (IRM) (2010). Kurumsal Risk Yönetimine Yapısal Bakış Açısı ve ISO 31000 Yükümlülükleri. London: The Institute of Risk Management.

Institute of Risk Management (IRM) (2018). *A Risk Practitioners Guide to ISO 31000: 2018*. United Kingdom, London: The Institute of Risk Management UK.

International Finance Corporation (IFC). (1999). *Corporate Governance Manuel*. Washington: Century Publishing Company.

Ittonen, K. (2010). A Theoretical Examination of the Role of Auditing and the Relevance of Audit Reports. *Proceedings of the University of Vaasa, Teaching Aid Series*. Finland: University of Vaasa.

İbiş, C. & Çatıkkaş, Ö. (2012). İşletmelerde İç Kontrol Sistemine Genel Bakış. *Sayıştay Dergisi*, 85, Nisan-Haziran, 95-121.

Jackson, R. (2007). Taking the High Road. *Internal Auditor*, April, 50-54.

Jefferson Wells (2009). *Internal audit from Corporate Policeman to Strategic Partner in GRC Success.* A White Paper. Milwaukee, United States: Jefferson Wells Inc.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of financial economics*, 3 (4), 305-360.

Johnstone, K., Gramling, A. A. & Rittenberg, L. E. (2014). *Auditing: a Risk-Based Approach to Conducting a Quality Audit*. Ohio: South-Western Cengage Learning.

Jöreskog, K. G., & Sörbom, D. (1996). *LISREL 8: User's reference guide*. Chicago, IL: Scientific Software International.

Kagermann, H., Kinney, W., Küting, K. & Weber, C. P. (2008). *Internal Audit Handbook Mangement with the SAP – Audit Roadmap*. Berlin, Heidelberg: Springer-Verlag.

Kara, S. & Sakarya, Ş. (2012). Kurumsal Risk Yönetimi Çerçevesinde Risk Odaklı İç Denetim ve İMKB Uygulaması. *Muhasebe ve Vergi Uygulamaları Dergisi*, 1, 69-95.

Karakaya, A. & Akbulut, H. (2010). Safranbolu'daki Turizm İşletmelerinde Kurumsal Yönetimin Uygulanabilirliğine Yönelik Bir Araştırma. *ZKÜ Sosyal Bilimler Dergisi*, 6 (11), 17-32.

Karakoç, F. Y., & Dönmez, L. (2014). Ölçek geliştirme çalışmalarında temel ilkeler. *TED*, 40(40).

Kavut, L., Taş, O. & Şavlı, T. (2009). *Uluslararası Denetim Standartları Kapsamında Bağımsız Denetim*. İstanbul: İSMMMO Yayınları, Yayın No:130.

Kell, W., Boynton, W. & Ziegler, R. (1989). *Modern Auditing (Fourth Edition)*, London: John Wiley & Sons Inc.

Knight, K.W. (2006). Risk management a journey not a destination. Paper presented at the *Executive Meeting 2006. 20th May 2006*, Brazil: Hotel Do Frade & Golf Resort, Angra Dos Reis.

Kepekçi, C. (1982). *İşletmelerde İç Kontrol Sisteminin Erkinliğini Sağlamada İç Denetimin Rolü.* Eskişehir: İktisadi ve Ticari İlimler Akademisi Yayınları, Yayın No: 251.

Kepekçi, C. (1994). *İç Kontrol Sistemi*. Ankara: TÜRMOB Temel Eğitim ve Staj Merkezi Yayınları.

Koçel, T. (2003). *İşletme Yöneticiliği*. İstanbul: Beta Basım Yayım.

KPMG (2014). Yönetişim Hizmetleri: GRC: Yüksek Performans ve Düşük Maliyet için Ortak Dil. İstanbul: Akis Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş.

KPMG (2017). *Top 10 Internal Audit Focus Areas For Technology Companies*. Whitepaper. United States of America, Delaware: KPMG LLP International.

Kral, R. (2009). Effective Corporate Compliance Programs. Governance Issue Newsletter, 4.

Kurnaz, N. & Çetinoğlu, T. (2010). *İç Denetim Güncel Yaklaşımlar*. Kocaeli: Umuttepe Yayınları.

Küçükkocaoğlu, G. & Küçüksözen, C. (2005). Gerçeğe Aykırı Finansal Tabloların Ortaya Çıkarılması: İmkb Şirketleri Üzerine Ampirik Bir Çalışma. *Muhasebe ve Finansman Dergisi*, 28 (4), s. 160-171.

Küpçü, H. (2011). *İç Denetim ve Kurumsal Yönetim*. Yayımlanmamış Doktora Tezi. Sakarya: Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, 28, 563–575.

Leftwich, A. (1993). Governance, the State and the Politics of Development. *Development and Change*, 25 (2), 363-386.

Limmroth, S. (2012). Internal Audit and Compliance as a Combined Function: Lessons Learned. *Journal of Health Care Compliance*. Eylül-Ekim, 27-32.

Limperg, Theodore (1985). *The Social Responsibility of the Auditor (A Basic Theory on the Auditor's Function by Professor Theodore Limperg (1879-1961) of the University of Amsterdam, with some recent comments)*. Amsterdam: Limperg Instituut.

Lvov, B. (2009). The three lines of defence. *KPMG*, 25, 1-4.

Lynford, G. (2015). *Internal control audit and compliance: documentation and testing under the new COSO framework*. New Jersey: JohnWiley & Sons Inc.

Maassen, G. F. (2002). *An international comparison of corporate governance models: a study on the formal independence and convergence of one-tier and two-tier corporate boards of directors in the Unites States of America, the United Kingdom and the Netherlands* (No. 31), Netherlands, Amsterdam: Spencer Stuart.

Madlener, J.J. (2009). *The Implications of Integrating Governance, Risk and Compliance in Business Intelligence Systems on Corporate Performance Management*. Erasmus MC: University Medical Center Rotterdam.

Mahzan, N. & Yan, C., M. (2014). Harnessing the benefits of Corporate Governance and Internal Audit: Advice to SME. *Procedia - Social and Behavioral Sciences*, 115, 156-165.

Mallin, C. A. (2013). *Corporate Governance (Four Edition).* United Kingdom: Oxford University Press.

Man, A., Schoevaart, M. & Wijk, H. (2010). *The internal auditor as spider in the GRC web 'Cooperating while maintaining independence'*. Amsterdam: NIVRA.

Manab, N. A., Kassim, I. & Hussin, M. R. (2010). Enterprise-Wide Risk Management (EWRM) Practices: Between Corporate Governance Compliance and Value Creation. *International Review of Business Research Papers*, 6 (2), July, 239 – 252.

Manifest Agency (2004). *Milestones in UK Corporate Governance*. London: Manifest the Proxy Voting Agency.

Marianne, L. J. (2006). Accounting Students' Knowledge and Perceptions of the Sarbanes-Oxley Act of 2002. *Academy of Educational Leadership Journal*, 10 (2), 1-24.

Marks, N. (2010). Defining GRC. *Internal Auditor*, February, 25-27.

Marks, N. (2013). Technology for Internal Auditors. *Internal Auditor*, August, 30-34.

Matyjewicz, G. & D'Arcangelo, J. R. (2004). ERM-based auditing. *Internal Auditing*, Kasım-Aralık, 4-18.

Mautz, R. K. & Sharaf, H. A. (1961). *The Philosophy of Auditing*. Florida: American Accounting Association, Monograph No:6.

McGartland R. D., Berg-Weger M., Tebb S. S., Lee E. S., Rauch, S. (2003): Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research*, 27 (2), pp. 94-104.

McClean, C. & Rasmussen, C. (2007). *The Forrester wave: Enterprise governance, risk, and compliance platforms*, Forrester Research. Q4, 1-22.

McNamee D. & Chan, S. (2002). E-Ticaret Riskini Anlamak. *İç Denetim*, Kış, 2, 38-39.

Ankara: Detay Yayıncılık.Mefford, J. (2016). The GRC Audit Quandary. *Compliance Week*, January, 42-43.

Menteş, A. (2009). *Kurumsal Yönetişim ve Türkiye Analizi*. İstanbul: Derin Yayınları.

Messier, F. W., Glover, S. M. & Prawitt, D. F. (2016). *Auditing & assurance services: a systematic approach.* New York: McGraw- Yayınları.

Meydan, C. H. Ş. Harun (2015). *Yapısal Eşitlik Modellemesi AMOS Uygulamaları.*

Mihret, D. G. & Admassu, M.A. (2011). Reliance of External Auditors on Internal Audit Work: A Corporate Governance Perspective. *International Business Research*, 4 (2), 67-79.

Milroy, P. (1995). Compliance And Internal Audit. *Journal of Financial Regulation and Compliance*, 3(3), 222-227.

Mitchell, S. (2007). GRC360: A framework to help organisations drive principled performance. *International Journal of Disclosure and Governance*, 4 (4), 279–296.

Mitchell, S. (2008). Governance, Risk and Compliance (GRC). Sean Lyons (Ed.) *Corporate Defense Insights: Dispatches from the Front Line* içinde (s. 68-75). Ireland: Q&A.

Mitchell, S. (2010). *Principled Performance & GRC*. Scottsdale, Arizona: OCEG.

Mitchell, S. & Switzer, C. (2016). *The Building Blocks of GRC: Visualizing an Effective Capability*. Scottsdale, Arizona: OCEG.

Moeller, R. & Witt, H., N. (1999). *Brink's Modern Internal Auditing (5th Ed)*. New York: John Wiley & Sons Inc.

Moeller, R. R. (2004). *Sarbanes-Oxley and the new internal auditing rules*. New Jersey: John Wiley & Sons.

Moeller, R. R. (2008). *Sarbanes-Oxley internal controls: effective auditing with AS5, CobiT and ITIL*. New Jersey: John Wiley & Sons.

Moeller, R. R. (2009). *Brink's modern internal auditing: a common body of knowledge.* New Jersey: John Wiley & Sons.

Moeller, R. (2011). *COSO Enterprise Risk Management: establishing effective governance, risk, and compliance processes*. New Jersey: John Wiley & Sons.

Mont, J. (2016). Parsing the Difference Between GRC & ERM. *Compliance Week*, January, 36-37.

Morris D. G. (2005). *An Accountant's Guide to Risk Management*. United Kingdom: Tottel Publishing.

Murray, A. (1976). The first internal auditors. *Journal of Accountancy*, January, 141, 98.

Namiri, K. & Stojanovic, N. (2007). A formal approach for internal controls compliance in business processes. *8th Workshop on business process modeling, development, and support proceedings*, Trondheim, Norway: Tapir Academic Press, 1-9.

OECD. (2005). *Kurumsal Yönetim Derneği Ekonomik İşbirliği ve Kalkınma Örgütü Kurumsal Yönetim İlkeleri*. Yayın No: KYD-Y/2005-01-01, İstanbul: TKYD.

Okay, B. (2005). Hepsi Bizim Günlük İşimiz. *TİDE İç Denetim*. Bahar, 16-19.

Open Compliance and Ethics Group (OCEG). (2009). *GRC capability model: Version 2.0 [achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance]*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2015a). *GRC capability model: Version 3.0 [achieving principled performance by integrating the governance, assurance and management of performance, risk and compliance]*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2015b). *Grc Maturity Survey How The Approach To GRC Strategy & Integration Affects Confidence*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2015c). *GRC Technology Solution Guide*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2016). *Critical Conversations CAE at the Center*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2017). *2017 GRC Metrics Survey*. Scottsdale, Arizona: OCEG.

Open Compliance and Ethics Group (OCEG). (2018). *Principled Performance Playbook: Controls Performance Verification*. Scottsdale, Arizona: OCEG.

O'Regan, D. (2003). *International Auditing: Practical Resource Guide*. New Jersey: John Wiley and Sons.

Önce, S. & İşgüden, B. (2012). İç Denetim Faaliyetinin Gelişen Ve Değişen Bilgi Teknolojileri Ortamı Açısından Değerlendirilmesi: İmkb–100 Örneği. *Yönetim ve Ekonomi Araştırmaları Dergisi*, 17, 38-70.

Özen, Y., & Gül, A. (2007). Sosyal ve eğitim bilimleri araştırmalarında evren-örneklem sorunu. *Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi Dergisi*, (15), 394-422.

Özeren, B. (2000). *İç Denetim, Standartları ve Mesleğin Yeni Açılımları*. Sayıştay Araştırma/İnceleme/Çeviri Dizisi: 8, Ankara: Sayıştay Yayın İşleri Müdürlüğü.

Özsoy, M. T. (2004). Risk Odaklı Denetim ABD Uygulaması ve Türkiye Açısından Değerlendirmesi. *Active Dergisi*, Mart-Nisan, 32-40.

Paape, L., Scheffe, J., & Snoep, P. (2003). The relationship between the internal audit function and corporate governance in the EU–a survey. *International Journal of Auditing*, 7(3), 247-262.

Pallant, J., & Manual, S. S. (2016). *A Step by Step Guide to Data Analysis using IBM SPSS*, 6th, USA: McGraw-Hill Education

Page, M., & Spira, L. F. (2004). *The Turnbull Report. Internal Control and Risk Management: The Developing Role of Internal Audit*. Edinburgh: The Institute of Chartered Accountants of Scotland.

Papazafeiropoulou, A. & Spanaki, K. (2015). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, 1-13.

Parkinson, M. (2018). COSO ERM: Integrating with Strategy and Performance. Asian Confederation IIA Conference 2018, 29-30 October 2018, Malaysia: Kuala Lumpur Convention Centre.

Peak, D. (2012). *Fundamentals Of Grc: The Connected Roles Of Internal Audit And Compliance*. Whitepaper, Toronto: Thomson Reuters Accelus.

Pehlivanlı, D. (2010). *Modern İç Denetim: Güncel İç Denetim Uygulamaları*. İstanbul: Beta Basım Yayım Dağıtım.

Pehlivanlı, D. (2015). *Yönetişim, Risk ve Uyum*. İstanbul: Beta Basım Yayım Dağıtım.

Pekel, A. (2008). *Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri*. Ankara: Türkiye Bilişim Derneği.

Pickett, K. H. S. (2010). *The İnternal Auditing Handbook*. West Sussex: John Wiley & Sons.

Pickett, K. H. S. (2011). *The Essential Guide to Internal Auditing*. West Sussex: John Wiley & Sons.

Pitt, S. A. (2014). *Internal Audit Quality: developing a quality assurance and improvement program*. New Jersey: John Wiley & Sons.

Price, J. C. (2006). ABD'de CPA'ların Karşılaştığı Sorunlar Meydan Okuyuşlar ve Fırsatlar. *Muhasebe Finansman Dergisi*, 29, Ocak, s.15-19.

Price Waterhouse Coopers (2004). *Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management*. A White Paper, London: PWC.

Price Waterhouse Coopers. (2005). *8th Annual Global Ceo Survey: Bold Ambitions,* Careful Choises. Boston: Merril Daniels.

Price Waterhouse Coopers (PWC) (2006). *Her Yönüyle Kurumsal Yönetim*. İstanbul: İnfomag Yayıncılık.

Prinsenberg, M. & Sluis, R. V. D. (2017). COSO Enterprise Risk Management Framework-Integrating Strategy and Performance. Netherlands, Den Bosch: PricewaterhouseCoopers.

Proctor, P.E. & Caldwell, F. (2011). *A Comparison Model for the GRC Marketplace 2011-2013*. Stamford: Gartner Report, ID: G0210517.

Protiviti. (2016). *Internal Auditing Around the World – Perpectives from Women in Audit Leadership Roles – How Technology is Impacting Internal Audit Functions*. New York: Protiviti Inc.

Ramamoorti, S. (2003). Chapter 1: Internal Auditing: History, Evaluation, and Prospects. *The Institute of Internal Auditors Research Foundation (IIARF), Research Opportunities in Internal Auditing* içinde (s. 1-23). Florida: The Institute of Internal Auditors.

Ramanathan, S. (2010). A Case for a Process-based Approach to GRC. *Isaca Journal*, 5, 1-5.

Racz, N., Weippl, E. & Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC). *11th IFIP TC 6/TC 11 International Conference for Communications and Multimedia Security*, s. 106-117, Linz, Austria, Mayıs-Haziran, 2010, ISBN: 9783642132414. Bart De Decker & Ingrid Schaumüller-Bichl (Eds.).

Rasmussen, M. (2009). An Enterprise GRC Framework. *Internal Auditor*, October, 61-65.

Ratliff, R., L. & Reding, K., F. (2002). *Introduction to Auditing: Logic, Principles, and Techniques*. Altamonte Springs, Florida: The Institute of Internal Auditors.

Raykov, T. & Marcoulides, G. A. (2006). *A First Course In Structural Equation Modeling*. Mahwah, NJ: Lawrence Erlbaum Associates.

Reding, F.K. Sobel, P. J. Anderson, L. U. Head, M. J. Ramamoorti, S. Salamasick, M. & Riddle, C. (2013). *Internal Auditing: Assurance&Consulting Services.* Altomonte Springs: The IIA Research Foundation.

Reeve, J., T. (1990). Internal Audit in the Year 2000. *Internal Auditor*, February 21-25.

Reezae, Z. & Riley, R. (2002). *Financial Statement Fraud, Prevention, and Detection*. Newyork: John Wiley &Sons, Second Editon.

Rezaee, Z., & Reinstein, A. (1998). The impact of emerging information technology on auditing. *Managerial Auditing Journal*, 13(8), 465-471.

Rezaee, Z., Olibe, K., O. & Minmier, G. (2003). Improving corporate governance: the role of audit committee disclosures. *Managerial Auditing Journal*, 18 (6/7), 530-537.

Richtermeyer, S. B. (2018). Enterprise Risk Management Integrating with Strategy and Performance. USA, Massachusetts: COSO.

Rishel, T. D., & Ivancevich, S. H. (2003). Additional opportunities for internal auditors in IT implementations. *Internal Auditing*, 18(2), 35-35.

Risk & Insurance Management Society (RIMS). (2012). *Risk Management and Internal Audit: Forging a Collaborative Alliance. Executive Report: The Risk Perspective.* Newyork: RIMS Press.

Risk Management Sub-group of the Basle Committee on Banking Supervision. (1998). *Framework for Internal Control Systems in Banking Organizations*. Basle: Basle Committee on Banking Supervision.

Rittenberg, L., & Anderson, D. (2002). Unleashing the potential of internal audit: as executives and directors rethink their corporate governance procedures, the authors offer a four-step approach to strengthening corporate assurance. *Financial Executive*, 18(7), 48-50.

Rosenau, J. (1992). Governance, Order and Change in World Politics, J. N. Rosenau & E. O. Czempiel (Ed.), *Governance without Government: Order and Challenge in World Politics* içinde (s. 1-19). Cambridge: Cambridge University Press.

Ruud, T. F. (2003). The internal audit function: An integral part of organizational governance. *Research opportunities in internal auditing*, 73-96.

Ruppert, M. P. (2006). Roles and Responsibilities – Corporate Compliance and Internal Audit. *Society of Corporate Compliance and Ethics*, 18, 1-5.

Salehi, M. (2011). Audit expectation gap: Concept, nature and trace. *African Journal of Business Management*, 5 (21), 8376-8392.

Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. *Managerial Auditing Journal*, 21(1), 63-80.

Sarens, G., Decaux, L & Lenz, R. (2012). *Combined Assurance, Case Studies on a Holistic Approach to Organizational Governance*. Amerika, Florida: The Institute of Internal Auditors Research Foundation.

Sawyer, L. B. (1993). Why Internal Auditing. *Internal Auditor*, 50 (6), 43-50.

Sawyer, L. B., Dittenhofer, M. A. & Scheiner, J. H. (2005). *Sawyer's İnternal Auditing. (5th Edition)*. Florida: The Institute of Internal Auditors.

Schneider, G. P., Sheikh, A. & Simione, K. A. (2012). Holistic Risk Management: An Expanded Role For Internal Auditors. *Academy of Accounting and Financial Studies Journal*, 16 (1), 25-34.

Schweik, A., L. & Watts, W., C. (2015). What Does the Future Hold for Internal Audit? *Crowe Horwath*, Nisan, 1-8.

Senal, S. & Aslantaş Ateş, B. (2019). Bütünleşik Güvence Yaklaşımı ve İç Denetimin Rolü. A. K. Uzun, G. Yurtsever ve E. Yenigün (Ed.) *Uluslararası Akademik Forum* içinde (s. 279-295). İstanbul: Türkiye İç Denetim Enstitüsü Yayınları (Yayın No:15).

Selim, G. & Mcnamee, D. (1999). The Risk Management and Internal Auditing Relationship: Developing and Validating a Model. *International Journal of Auditing*, 3, 159-174.

Sermaye Piyasası Kurulu (SPK) (2005). *Sermaye Piyasası Kurulu Kurumsal Yönetim İlkeleri*, Ankara: Sermaye Piyasası Kurulu.

Silverman, M. (2008). *Compliance Management for Public, Private, or Non-Profit Organizations*. Amerika, New York: McGraw-Hill Companies, Inc.

Shaim, A., Batenburg, R., Djwalapersad, R. & Pennings, T. (2014). *A healthcare view on Governance, Risk Management & Compliance (GRC)*. Amsterdam, Netherlands: Atos Consulting.

Shortreed, J., Fraser, J., & Purdy, G. (2011). The Future Role of Internal Audit in (Enterprise) Risk Management. Institute of Internal Auditors Research Foundation's (IIARF's) *Internal Auditing's Role in Risk Management*, March, 1-
Smith, A. (1838). *An inquiry into the nature and causes of the wealth of nations*. London: Ward, Lock & Tyler.

Sobel, P. J. (2018). COSO ERM: Integrating with Strategy and Performance. The Institute of Internal Auditors International Conferance, UAE, Dubai, 6-9 Mayıs 2018.

Soltani, B. (2007). *Auditing: an International Approach*. London: Hill Education.

Spira, L. F. & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16 (4), 640-661.

Steinberg, R. (2011). *Governance, Risk Management, and Compliance It Can't Happen to Us-Avoiding Corporate Disaster While Driving Success*. Amerika, New Jersey: John Wiley & Sons Inc.

Suwaidan, M. S. ve Qasım, A. (2010). External Auditors Reliance on Internal Auditors and Its Impact on Fees: An Empirical Investigation. *Managerial Auditing Journal*, 25 (6), 509-525.

Swanson, D. (2006). Auditing Ethics and Compliance Programs. *Compliance Week*, June, 1-6.

Swanson, D. (2010). *Swanson on Internal Auditing Raising the Bar*. Cambridgeshire, United Kingdom: IT Governance Publishing.

Switzer, C. S., Suri, A., Kapoor, G. & Nazemoff, V. (2013). Governance, risk management, and compliance: creating the right grc strategy for your company. *Books24x7 ExecBlueprints*, 1-24.

Switzer, C., Delmar, Y. & Quinlan, P. (2015). Performing GRC Actions and Controls. *Compliance Week*, November, 1-2.

Switzer. C. (2015). Let's Change the Way We Talk About Controls. *Compliance Week*, November, 50.

Switzer, S. (2007). *Internal audit reports post Sarbanes-Oxley: a guide to process-driven reporting*. New Jersey: John Wiley & Sons.

Şakar, N. (2013). Yetki, Güç ve Yetki Devri. C. Koparal ve İ. Özalp (Ed.) *Yönetim ve Organizasyon* içinde (s.70-93). Eskişehir: Anadolu Üniversitesi, Açıköğretim Fakültesi Yayınları.

Şehirli, K. (1999). *Kurumsal Yönetim*. Sermaye Piyasası Kurulu Araştırma Raporu. Ankara: SPK Denetleme Dairesi.

Şen, E. (2013). *Kurumsallaşma İle Firma Performansı İlişkisinde Kurumsal Yönetişimin Rolü*. Yayımlanmamış Doktora Tezi. Kocaeli: Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü.

Şimşek, Ö. F. (2007). *Yapısal Eşitlik Modellemesine Giriş: Temel İlkeler ve LISREL Uygulamaları*. Ankara: Ekinoks.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics* (sixth ed.) Boston: Pearson.

Tabuena, J. (2010). Why GRC Matters to the Internal Auditor. *Compliance Week*, September, 1-6.

Tadewald, J. (2014). GRC Integration: A Conceptual Foundation Model for Success. *Management Accounting Quartely*, 15 (3), 10-18.

Tarantino, A. (2008). *Governance, Risk, and Compliance Handbook Technology, Finance, Environmental, and International Guidance and Best Practices*. New Jersey: John Wiley & Sons.

Taşçı, K. & Yılmaz, Ö. (2013). Kurumsal Süreç Etkinliğinde Bilgi Teknolojileri Temelli İç Kontrol Sistemlerinin Önemi. Mevzuat Dergisi, 14 (161).

Taşkın, Ç. & Akat, Ö. (2010). Araştırma Yöntemlerinde Yapısal Eşitlik Modelleme. Bursa: Ekin Yayınevi.

Tavşancıl, E. (2002). Tutumların Ölçülmesi ve SPSS ile Veri Analizi. Ankara: Nobel Yayınevi.

Thomson Reuters Accelus (2012). Fundamentals of Grc: The Connected Roles of Internal Audit And Compliance. Whitepaper. Kanada, Toronto: Thomson Reuters Publications.

Tillinghast-Tillinghast, P. T. (2004). *Adding value through risk and capital management*. New York: Tillinghast-Towers Perrin.

Tuan, K. (2015). İç Denetçi ve Bağımsız Denetçi Arasındaki Koordinasyon ve İşbirliğinin Denetim Standartları Açısından Değerlendirilmesi. *Akademik Sosyal Araştırmalar Dergisi*, 3 (18), 319-329.

Tuzcu, A. (2004). *Halka Açık Şirketlerde Kurumsal Yönetim Anlayışı İMKB-100 Örneği*. Ankara: Turhan Kitabevi.

Tüm, K. (2013). Kurumsal Yönetim, İç Denetim ve İç Denetimin Kalitesi: Kalite Güvence ve Geliştirme Programı. *Çukurova Üniversitesi İİBF Dergisi*, 17 (2), 93-112.

Türedi, H., Karakaya, G. & İldem, M. (2015). Kurumsal Yönetim ve İç Denetim İlişkisi. *Sayıştay Dergisi*, 96, Ocak-Mart, 55-74.

Türedi, H., Koban, A. O. & Karakaya, G. (2015). Coso İç Kontrol (Abd) Modeli İle İngiliz (Turnbull) ve Kanada (Coco) Modellerinin Karşılaştırılması. *Sayıştay Dergisi*, 99, Ekim-Aralık, 95-119.

Türk Sanayicileri ve İşadamları Derneği (TÜSİAD). (2002). *Kurumsal Yönetim En iyi Uygulama Kodu: Yönetim Kurulunun Yapısı ve İşleyişi*. Yayın No. TÜSİAD-T/ 2002-12/336, İstanbul: Lebib Yalkın Yayımları ve Basım İşleri.

Türk Sanayicileri ve İşadamları Derneği (TÜSİAD). (2008). *Yönetim Kurulları'nda İç Denetim Hakkında Sorulması Gereken 12 Soru*. Yayın No: TÜSİAD-T/2008-05-461, İstanbul: Graphis Matbaa.

Türkiye Kurumsal Yönetim Derneği (TKYD) (2011). *Ekonomi Gazeteciliği için Kurumsal Yönetim El Kitabı*. İstanbul: TKYD Yayınları.

TÜSİAD (2012). *Uygulama Örnekleri ile Birlikte A-.Z'ye Denetim Komiteleri*. Yayın No: Tüsiad-T/2012-06/527, İstanbul: Sis Matbaacılık.

Uluslararası İç Denetçiler Enstitüsü (IIA). (2009). *IIA Pozisyon Raporu: İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol*. İstanbul: Türkiye İç Denetim Enstitüsü.

Usul, H., Titiz, İ., & Burcu, A. (2011). İç Kontrol Sisteminin Kurumsal Yönetimin Oluşumundaki Etkinliği: Marmara Bölgesi Belediye İşletmelerine Yönelik Bir Uygulama. *Muhasebe ve Finansman Dergisi*, (49).

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

Uzay, Ş. (2003). İç Denetimin Geleceği ve Yeni Eğilimler. *22. Türkiye Muhasebe Eğitimi Sempozyumu*'nda sunulan bildiri. Antalya: 21-25 Mayıs.

Uzun, A. K. (2010). *Kurumsal Yönetim ve İç Denetimin Kalite Güvencesi*. İstanbul: Deloitte Türkiye.

Uzun, A. K. (2011). Kurumsal Risk Yönetimi ve İç Denetim. *Önce Kalite Dergisi*, Mart-Nisan, 151, 26-29.

Uzun, A. K. (2012). İç Denetim. M. Erdoğan (Ed.) *Denetim* içinde (s. 78-103). Eskişehir: Anadolu Üniversitesi, Açıköğretim Fakültesi Yayınları.

Uzunay, V. (2007). *Control Objectives for Information and related Technology*. Ankara: İç Kontrol Merkezi Uyumlaştırma Dairesi.

Veneziano L. & Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21(1):67-70.

Vicente, P. & Da Silva, M. M. (2011). A Conceptual Model for Integrated Governance, Risk and Compliance. *Advanced Information Systems Engineering*, 6741, 199–213.

Vicente, P., Racz, N., & Da Silva, M. M. (2012). *Towards a Reference Model for Integrated Governance, Risk and Compliance*. Portugal: Instituto Superior Tecnico, Universidade Tecnica de Lisboa.

Volosin, E. (2007). *The theories of audit expectations and the expectations gap*. Münih: GRIN Verlag.

Walker, P. L., Shenkir, W. G., & Barton, T. L. (2002). *Enterprise risk management: pulling it all together*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Walker P., L., Shenkir W., G. & Barton T., L. (2003). ERM in Practise. *Internal Auditor*, August. 60 (4), 51-55.

Wood, D. A. (2004). *Increasing Value through Internal and External Auditor Coordination*. (Prepared for the IIA Research Foundation Esther R. Sawyer Scholarship Award) Florida: The IIA Research Foundation.

Wu, T. H., Huang, S. M., Huang, S. Y., ve Yen, D. C. (2016). The effect of competencies, team problem-solving ability, and computer audit activity on internal audit performance. *Information Systems Frontiers*, 1-16.

Yavuz, S. T. (2002). İç Kontrol Sisteminin Bileşenleri. *Bankacılar Dergisi*, 42, 39-57.

Yaşlıoğlu, M. M. (2017). Sosyal bilimlerde faktör analizi ve geçerlilik: Keşfedici ve doğrulayıcı faktör analizlerinin kullanılması. *Istanbul Business Research, 46*, 74-85.

Yenigün, T. (2008). *Kurumsal Yönetim ve İşletme İçi Denetim*. Yayımlanmamış Doktora/Yüksek Lisans Tezi. İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü.

Yetiş, A. (2001). Kurum Çapında Entegre Risk Yönetiminin Teknolojik Bileşenleri. *Deloitte Risk Yönetimi Haber Bülteni*, Mayıs/Haziran, 3.

Yılancı, M. (2003). *İç Denetim (Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma)*. Yayın No: 86, Eskişehir: Osmangazi Üniversitesi Yayınları.

Yıldırım, O., Dalgeç, A. & Özkol, E. (1995). *Muhasebenin Tarihsel ve Çağdaş Konumlarından Geleceğine Bakış*. Yayın No:23, Ankara: TÜRMOB Yayınları.

Yıldız, B. (2019). Sürekli Denetim Teknolojisi. A. K. Uzun, G. Yurtsever ve E. Yenigün (Ed.) *Uluslararası Akademik Forum* içinde (s. 279-295). İstanbul: Türkiye İç Denetim Enstitüsü Yayınları (Yayın No:15).

Yılmaz, V., Çelik, H. E. & Ekiz, E. (2006). Investigation of the Factors Affecting Loyalty to Organization through The Structural Equation Modeling- Example from Private and Public Banks. *Anadolu University Journal of Social Sciences*, 6, 171-184.

Yurdugül, H. (2005). Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması. *XIV. Ulusal Eğitim Bilimleri Kongresi*, 1, 771-774.

Yurtsever, G. (2008). *Bankacılığımızda iç kontrol*. İstanbul: Türkiye Bankalar Birliği.

Zwaan, L. D., Stewart, J. ve Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, 26 (7), 586 – 604.

https://www.ahia.org/assets/Uploads/pdfUpload/WhitePapers/AuditCompliance-RolesResp04052006.pdf (Erişim Tarihi: 04.07.2017).

https://www.aicpa.org/research/standards/auditattest/sas.html (Erişim Tarihi: 11.02.2017).

http://www.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/CEI/2015/804_2.pdf (Erişim Tarihi: 17.02.2017).

http://www.corporatecomplianceinsights.com/2017-a-transformational-year-for-grc/ (Erişim Tarihi: 22.10.2016).

http://www.denetimnet.net/UserFiles/Documents/DenetcininNotDefteri/Turkey-tr_kys_GenelKurulunveYonetimKurulununKarsilikliKonumu_021208.pdf. (Erişim Tarihi: 04.04.2017).

http://files.shareholder.com/downloads/MAN/0x0x319890/2cc71040-4037-4f54-9fff-db11163312e5/InternalAu2.pdf. (Erişim Tarihi: 17.06.2017).

https://www.gartner.com/en/information-technology/ciso (Erişim Tarihi: 16.02.2017).

http://www.iia.nl/Sitefiles/Downloads/Fundamentals_of%20GRC_Internal_Audit_and_Compliance_US.pdf. (Erişim Tarihi: 22.06.2017).

https://www.isaca.org/COBIT/Documents/An-Introduction.pdf (Erişim Tarihi: 28.10.2016).

http://www.oceg.org/grc-glossary/ (Erişim Tarihi: 04.11.2016).

http://www.oceg.org/resources/illustration-how-do-we-make-the-business-case-for-integrated-grc-updated/ (Erişim Tarihi: 16.01.2016).

http://www.oceg.org/event/chief-audit-executive-talking-grc/ (Erişim Tarihi: 19.02.2017)

https://www.sap.com/solution/platform-technology/analytics/grc.html (Erişim Tarihi: 04.01.2017).

https://www.schneiderdowns.com/our-thoughts-on/risk-advisory-Internal/internal-audit-vs-compliance (Erişim Tarihi: 11.04.2017).

https://www.socscistatistics.com/effectsize/default3.aspx (Erişim Tarihi: 11.01.2019).

www.theiia.org/download.cfm?file=66127. (Erişim Tarihi: 07.05.2017).

https://www.tide.org.tr/page.aspx?nm=etik_kurallar (Erişim Tarihi: 02.10.2016).

http://www.tkyd.org/files/downloads/faaliyet_alanlari/yayinlarimiz/tkyd_yayinlari/nedir_bu_kurumsal_yonetim.pdf. (Erişim Tarihi: 07.03.2017)

# EKLER

**EK-1** VERİ TOPLAMA ARACI

**EK-2** MADDE HAVUZU DEĞERLENDİRME ÇALIŞMASI

**EK-3** İÇ DENETİMİN SORUMLULUKLARI ÖLÇEĞİ KOVARYANS MATRİSİ

**EK-4** YRU YAKLAŞIMININ FAYDALARI ÖLÇEĞİ KOVARYANS MATRİSİ

EK-1

Değerli Katılımcı,
Bu anket formu bir doktora tez çalışması kapsamında iç denetçinin Yönetişim-Risk-Uygunluk (YRU) Yaklaşımına ilişkin sorumluluklarını araştırmak üzere hazırlanmıştır. YRU (GRC); strateji, süreçler, teknoloji ve çalışanların düzenlenmesiyle işletmenin etik olarak doğru hareket etmesini ve risk yaklaşımı, iç politikalar ve dış düzenlemeler ile uyumlu olmasını sağlayan, böylece etkinliği ve verimliliği geliştiren işletme çapında yönetişim, risk ve uygunluğu sağlamayı amaçlayan bilgi teknolojileri tabanlı bütüncül bir yaklaşımdır. Vereceğiniz yanıtlar sadece bilimsel çalışma kapsamında değerlendirilecek olup bireysel düzeyde bir analiz yapılmayacaktır. Soruların doğru, eksiksiz ve içtenlikle doldurulması konusunda elinizden gelen hassasiyeti göstermeniz, çalışmanın nesnelliği için büyük önem taşır. İlgi ve katkınız için teşekkür ederiz.

Araş. Gör. Ahmet ONAY — Araştırmacı
Prof. Dr. Melih ERDOĞAN — Akademik Danışman

**Cinsiyetiniz:** Kadın (☐) Erkek (☐) **Yaşınız** : …….. **Mesleki deneyim (yıl)**: ……
**Unvanınız:** İç Denetçi(☐) Bağımsız Denetçi(☐) İşletme Yöneticisi(☐)
**İşletmenizde kullandığınız risk yönetimi modelini yazınız: ……..**
**YRU yaklaşımı hakkında anketi doldurmadan önce bilgi sahibi miydiniz? (Evet/Hayır).....**

**İç denetimin sorumluluklarına ilişkin sunulan ifadelere katılım düzeyinizi belirtiniz.**

| **İç Denetimin Yönetişim Sorumlulukları** | **OLMASI GEREKEN** | | | | | **UYGULAMADA** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **KesinlikleKatılmıyoru** | **Katılmıyorum** | **Kararsızım** | **Katılıyorum** | **KesinlikleKatılıyorum** | **Hiçbir Zaman** | **Nadiren** | **Bazen** | **Sık Sık** | **Her Zaman** |
| **İç Denetçi;** | | | | | | | | | | |
| YRU faaliyet sonuçlarının ölçülebilir olmasını sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU süreçlerini geliştirmek amacıyla yetkin personel transferi yapılmasını sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Üçüncü savunma hattındaki pozisyonu gereği bağımsızlığını korur. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletmede yönetişimi geliştirecek politika, yordam ve süreçlerin geliştirilmesine destek olur. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Yöneticilerin işletme paydaşlarına hesap verebilirliğini sağlayan mekanizmaları geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Birim yöneticileri ve üst yönetim arasında etkileşimi geliştirerek YRU çalışmalarını geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Çalışanların performansının ölçülebilmesi amacıyla doğru ölçütlerin belirlenmesinde yönetime rehberlik eder. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| İç kontrol, uygunluk, risk yönetimi, bağımsız denetim gibi güvence çalışanlarıyla koordinasyonu sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU yaklaşımını desteklemek amacıyla iç kontrol, risk yönetimi, yönetişim, sürdürülebilirlik gibi konularda çerçeve ve rehberleri bilir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

**İç Denetimin Risk Yönetimi Sorumlulukları**

| | OLMASI GEREKEN | | | | | UYGULAMADA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **İç Denetçi;** | **Kesinlikle Katılmıyorum** | **Katılmıyorum** | **Kararsızım** | **Katılıyorum** | **Kesinlikle Katılıyorum** | **Hiçbir Zaman** | **Nadiren** | **Bazen** | **Sık Sık** | **Her Zaman** |
| Risklerin doğru değerlendirildiğine ilişkin güvence sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Temel risklerin üst yönetim tarafından yönetilip yönetilmediğini inceler. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Risklerin değerlendirilmesinde üst yönetime rehberlik eder. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Kurumsal risk yönetimi faaliyetlerinde koordinasyonu sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Riskler hakkında konsolide raporlar hazırlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Kurumsal risk yönetimi çerçevesinin devamlılığını ve gelişimini sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletmenin risk iştahını ayarlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Risk yönetimi süreçlerini düzenler. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Üst yönetimin risk yönetimi çalışmalarında etkinliğini garanti eder. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletmede risk yönetiminin sorumluluğunu üstlenir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| İkinci savunma hattında bulunan risk ve kontrol birimlerinin etkinliğini geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Riskin tartışılması için ortak bir çerçevenin ve ortak bir dilin kullanılmasına katkı sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Risklere karşı uygulanacak eylemleri yönetim adına uygular. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Yönetim kurulunun onayına sunmak için kurumsal risk yönetimi stratejisini geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

**İç Denetimin Uygunluk Sorumlulukları**

| **İç Denetçi;** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Yapılması istenen davranışların teşvik edilmesi amacıyla davranış kuralları ve kodlar hazırlar. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Çalışanların yetki alanları içinde hareket etmelerini teşvik eden uygunluk kültürünü geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Yerel ve uluslararası düzenlemeleri göz önünde bulundurur. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Uygunluk ile ilgili öneriler geliştirir, gerektiğinde eğitimler verir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Uygunluk politikalarının geliştirilmesine destek olur. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Uygunluğu şeklen yasa ve düzenlemelerin yerine getirilmesinden daha fazlası olarak görür. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletme çalışanlarının uygunluk amaçlarını destekleyip desteklemediğini değerlendirir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletme faaliyetleri ile ilgili düzenli olarak uygunluk risk değerlendirmesi yapar. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İş süreçlerinin uygunluk amaçlarıyla tutarlı hale getirilmesine rehberlik eder. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Ulusal ve uluslararası düzenlemelerin takip edilmesini için kontrol yordamları geliştirir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Yasa ve düzenlemeler kaynaklı gereklilikleri izlemek için sistemler kurulmasını sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Uygunluğu test eden incelemelere denetim programında yer verir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletme birimleri arasında uygunluk programlarının tutarlılığı için çaba gösterir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |

| **İç Denetimin <u>Bilgi Teknolojileri</u> Sorumlulukları** | **OLMASI GEREKEN** | | | | | | **UYGULAMADA** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Kesinlikle Katılmıyorum** | **Katılmıyorum** | **Kararsızım** | **Katılıyorum** | **Kesinlikle Katılıyorum** | | **Hiçbir Zaman** | **Nadiren** | **Bazen** | **Sık Sık** | **Her Zaman** |
| **İç Denetçi;** | | | | | | | | | | | |
| YRU yazılımları üzerinde etkin kontrollerin oluşturulmasına danışmanlık yapar. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU yazılımlarının tasarımını ve işleyişini düzenli olarak gözden geçirir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İç kontrolün bilgi teknolojileri (BT) ortamında yürütülmesi için BT uzmanlarını gerektiği gibi yönlendirebilecek seviyede yazılım bilgisine sahiptir. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU yaklaşımı doğrultusunda birden fazla amaca hizmet eden kontroller geliştirmeye çalışır. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU yazılımının seçimi ve işletmeye adaptasyonu sürecinde üst yönetime rehberlik eder. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| YRU yazılımlarının amaçlar doğrultusunda geliştirilmesi için BT uzmanlarıyla işbirliği yapar. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sürekli denetimi sağlayan teknolojileri bilir ve kullanımını teşvik eder. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| Uygunluk faaliyetlerinin merkezileştirilmesini kolaylaştıran teknolojik çözümler konusunda danışmanlık yapar. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletmede sürekli denetim için otomatik kontrol modellerinin uygulanmasına destek olur. | ☐ | ☐ | ☐ | ☐ | ☐ | | ☐ | ☐ | ☐ | ☐ | ☐ |

**YRU Yaklaşımının İşletmeye Faydaları**

| **YRU Yaklaşımı;** | **Kesinlikle Katılmıyorum** | **Katılmıyorum** | **Kararsızım** | **Katılıyorum** | **Kesinlikle Katılıyorum** |
|---|---|---|---|---|---|
| İşletmede sürekli denetim ve izleme faaliyetlerinin geliştirilmesini sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |
| İş süreçlerinde bilginin kalitesini artırır. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Riske maruz kalma potansiyeli yüksek işletmelere daha fazla katma değer sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletme faaliyetlerinin kalitesini artırır. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Sayesinde elde edilen faydalar, YRU yaklaşımını uygulamanın maliyetinden yüksektir. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Risk yönetimini işletmeye değer katan bir faaliyete dönüştürür. | ☐ | ☐ | ☐ | ☐ | ☐ |
| İşletmenin risklere ve fırsatlara zamanında karşılık verebilmesini sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Yasa ve düzenlemelerin dayattığı zorunluluklara uyum sağlamayı kolaylaştırır. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Ortak dil, süreç ve teknoloji kullanımı ile iş süreçlerinin maliyetini azaltır. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Paydaşların beklentilerinin anlaşılmasını ve bunlara öncelik verilmesini sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Stratejik planlamanın risk bilinciyle oluşturulmasını sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |
| Örgüt kültürünün yaygınlaştırılmasına katkı sağlar. | ☐ | ☐ | ☐ | ☐ | ☐ |

Sabır gösterip anketimizi tamamlayarak çalışmamıza verdiğiniz destek için çok teşekkür ederiz.

EK-2

**YÖNETİŞİM-RİSK-UYGUNLUK (YRU) SORUMLULUKLAR VE UYGULAMALAR (YRU-SU) ANKETİ MADDE HAVUZU DEĞERLENDİRME ÇALIŞMASI**

**Sayın Alan Uzmanı,** doktora tezimde kullanacağım ölçek geliştirme çalışmasına destek vermeyi kabul ettiğiniz için çok teşekkür ederim. Çalışmada vereceğiniz cevaplar sadece akademik amaçlarla kullanılacaktır ve bireysel değerlendirmeye tabi tutulmayacaktır. Akademik hayatın en önemli basamağı olan doktora çalışmam için soruların içtenlikle doldurulması konusunda elinizden gelen hassasiyeti göstermenizi rica ederim. Soruların hassasiyetle gözden geçirilmesi çalışmanın kalitesine doğrudan katkı sağlayacaktır. Alan uzmanı olarak sunduğunuz değerli katkılarınız ve bilimsel desteğiniz için şimdiden çok teşekkür ederiz.

Danışman: Prof. Dr. Melih ERDOĞAN, Tez Öğrencisi: Ar. Gör. Ahmet ONAY

**YÖNERGE**

**Sayın Alan Uzmanı,**

Madde revizyonu süreci sırasında, sizden beklenenler aşağıda listelenmiştir:

1. Ölçülmesi hedeflenen olguya ilişkin geliştirilen her bir maddeyi belirtilen kapsamı dikkate alarak değerlendiriniz. Bunun için her bir maddenin konuyla ne kadar ilişkili olduğu belirtilmelidir.
2. Madde yazım kılavuzunu dikkate alarak ölçek maddelerinin anlaşılırlığını ve uzunluğunu değerlendiriniz.
3. Ölçülmek istenen yapıya ilişkin varsa yeni maddeler önerebilirsiniz.

**Madde Yazım Kılavuzu**

**1. Maddeler ölçülen olgunun içeriğini yansıtmalıdır.**

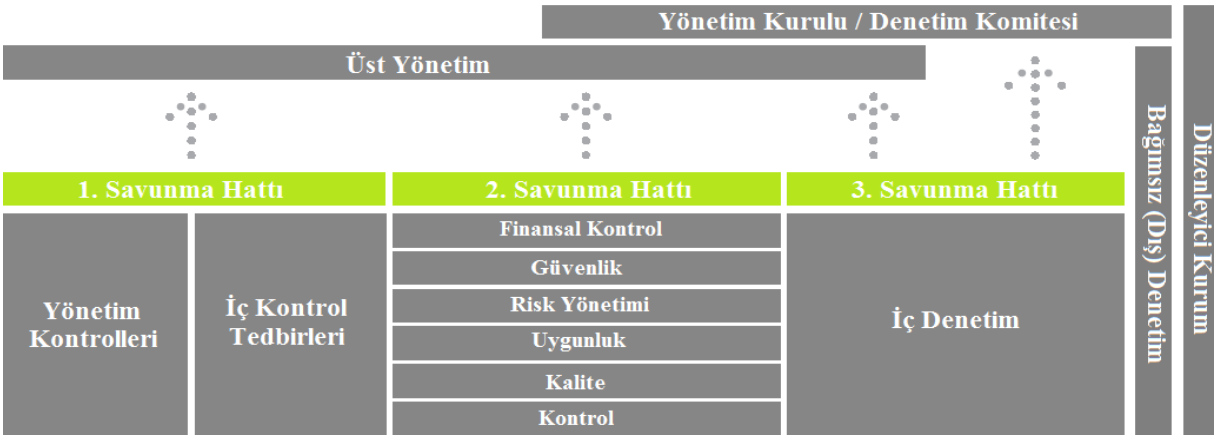
YRU-SU (Yönetişim-Risk-Uygunluk (YRU) Sorumluluklar ve Uygulamalar) anketinin amacı; öncelikli olarak iç denetçilere, bağımsız denetçilere ve şirket yöneticilerine göre yönetişim-risk-uygunluk (YRU) konusunda iç denetçilerin üstlenmesi gereken sorumlulukların belirlenmesi, sonrasında da mevcut uygulamalar ile tespit edilen sorumluluklar arasında farklılıklar olup olmadığının belirlenmesi amacıyla veri toplamaktır. İç denetçilerin üstlenmesi gereken sorumlulukları ve mevcut uygulamaları tespit etmek amacıyla aynı maddeler kullanılmıştır. Anketin bir diğer amacı da, uygulayıcılara (İç denetçiler, bağımsız denetçiler ve işletme yöneticileri) göre YRU yaklaşımının işletme faaliyetleri üzerinde olumlu etkisinin olup olmadığının belirlenmesidir.

**Tanımlar**

**Kurumsal Risk Yönetimi (KRY):** Kurumun hedeflerine ulaşmasını etkileyen fırsatlar ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için kurum çapında uygulanan, özel yapılandırılmış, istikrarlı, tutarlı ve kesintisiz bir süreçtir.

**Üç Hatlı Savunma Modeli:** Üç hatlı savunma modelinde, yönetim kontrolleri savunmanın birinci hattı, yönetim tarafından kurulan çeşitli risk, kontrol ve uygunluk gözetim birimleri savunmanın ikinci hattı ve bağımsız güvence yani iç denetim üçüncü hattı oluşturur. Bu üç hattın her biri işletmenin genişleyen yönetişim çerçevesinde açık bir rol oynar.

Üç hattın her biri, işletmenin yönetişim çerçevesinde belirgin bir rol oynamaktadır. Her bir hat kendi rolünü yerine getirdiğinde, işletme genel amaçlarında başarıya ulaşabilecektir.




**Yönetişim-Risk-Uygunluk (YRU):** Açık Uygunluk Etik Grubu (OCEG) YRU sözlüğündeki tanıma göre YRU bir organizasyonun dürüstlükle hareket ederken (uygunluk) ve belirsizliği ortadan kaldırırken (risk yönetimi) amaçlarına güvenilir bir biçimde ulaşmasına olanak tanıyan (yönetişim) yeteneklerin bütünleşik olarak bir araya getirilmesidir. YRU yönetişim, güvence, performans yönetimi, risk ve uygunluğu kapsar.

Racz vd. (2010) yaptıkları çalışmada literatür incelemesi ve çevrimiçi uzman anketi aracılığıyla kapsamlı bir YRU tanımı türetmiştir: YRU; strateji, süreçler, teknoloji ve çalışanların düzenlenmesiyle işletmenin etik olarak doğru hareket etmesini ve risk yaklaşımı, iç politikalar ve dış düzenlemeler ile uyumlu olmasını sağlayan, böylece etkinliği ve verimliliği geliştiren işletme çapında yönetişim, risk ve uygunluğu sağlamayı amaçlayan bütünleşik, bütüncül bir yaklaşımdır.

YRU, bakış açısına bağlı olarak farklı anlamları ya da bu anlamların hepsini birden ifade edebilen kapsamlı bir kavramdır. (1) YRU işletmenin yönetişim, risk yönetimi ve uygunluk yönetimi süreçlerini bir arada düşünen ve bu şekilde hem kaynakların daha etkin kullanılmasını hem de rekabet avantajı sağlamayı öngören bir yaklaşım, yönetim disiplini, anlayış ya da felsefedir. (2) Bu yaklaşımın işletmelerde daha kolay ve anlaşılır şekilde uygulanması için kullanılan bir çerçevedir. Aynı zamanda da (3) YRU yaklaşımının işletmelerde uygulanması için gereken teknik altyapıyı sunmak için geliştirilen bir teknoloji çözümüdür.

**Risk İştahı:** İşletme çapında bir bakış açısıyla, işletmenin kabul etmeye istekli olduğu risk miktarını yansıtır. İşletmenin almayı kabullendiği risk oranıdır ve işletmenin risk yönetim felsefesini yansıtır.

**Risk Toleransı:** İşletme amaçlarına ulaşılması konusunda kabul edilebilir fark seviyesidir. Toleranslar bir işletmenin her seviyedeki riskleri kabul edip etmeyeceğini değerlendirirken kullanması gereken rehberler ve ölçülerdir.

**Uygunluk:** Yasalar ve düzenlemeler tarafından tanımlanan zorunlu gerekliliklere ve sözleşme yükümlülüklerinden ve iç politikalardan kaynaklanan gönüllü gerekliliklere bağlı kalarak hareket etmeyi ve bağlı kalmak için sahip olunması gereken yeteneği ifade eder.

**Yönetişim:** İşletme tarafından yönlendirilen ve kontrol edilen kültür, değerler, misyon, yapı, politikalar ve tedbirlerdir. Bu bağlamda, yönetişim, yönetim kurulunun tüm faaliyetlerini kapsar. Ayrıca işletmenin çeşitli seviyelerinde bulunan yönetişim organları da yönetişim için önemli rol oynar.

**2. Maddelerin Anlaşılırlığı ve Uzunluğu**

**A. Madde Sayısı:** Ölçek geliştirmenin ilk aşamasında madde havuzu için çok sayıda madde üretilmiştir. Sizlerin katkılarıyla geliştirilen bu madde havuzundan en uygun ve ölçülebilir maddeler seçilecektir.

**B. Açık İfade Etme (Anlaşılabilirlik):** İyi bir madde tüm katılımcılar tarafından aynı şekilde anlaşılması noktasında net (açık) bir şekilde ifade edilmiş olmalıdır. Aşağıda iyi ve kötü maddelerin ayrıştırılmasında kullanılan bazı özellikler yer almaktadır.

- ***Okuma Zorluğu***: Hedef kitlenin düzeyine hitap eden ortak bir dil kullanılmış olmalıdır.
- ***Maddenin Uzunluğu***: Madde hedef kitlenin düzeyine bakılmaksızın kısa ve anlaşılır olmalıdır. Uzunluk, karmaşıklığı artırır, dolayısıyla anlaşılırlığı azaltır.
- ***Jargon kullanmaktan kaçının***. Hedef kitle de dikkate alınarak, ifadelerde aşırı teknik terimler kullanılmamalıdır.
- ***İki yönlü (çift namlulu) ifadelerden kaçının***. *Aynı ifadenin içinde* birden fazla konu olmamalıdır. Genellikle bu ifadeler 've', 'veya' bağlaçlarını barındırır. Bu tür ifadelerden kaçınılmalıdır. Örneğin, 'Maaşımı zamanında ve tam olarak alıyorum' ifadesine katılımcı görüşünü belirtirken hangi durumu dikkate alacağını kestiremeyebilir. Maaşını tam alan biri zamanında alamıyor veya zamanında alan biri tam bir maaş almıyor olabilir. Ya da "Ne param ne de zamanım var" ifadesi katılımcının yanıt vermesini zorlaştırabilir.
- ***Birden çok olumsuzlama ifadelerinden kaçının***. Çift negatif ifade, aynı cümlede iki olumsuzluk biçimi kullanıldığında ortaya çıkan bir dilbilgisi yapısıdır. Birden çok olumsuzlama ise, bir maddedeki birden fazla negatif olaya işaret eden daha genel bir terimdir. Bazı dillerde, çift negatifler birbirlerini iptal eder ve olumlu yargılar/durumlar üretirler; bazı dillerde ise, iki katına çıkan negatifler olumsuzlamayı yoğunlaştırmaktadır. Karmaşıklığı artırdığı ve anlaşılırlığı azalttığı için, birden çok olumsuzlama içeren ifadelerden kaçınılmalıdır. Örneğin, "Zamanımın olmadığını düşünmüyorum" ifadesi anlaşılmayı zorlaştırmaktadır.
- ***Hangi ismi nitelediği anlaşılmayan zamirleri kullanmaktan kaçının***. Örneğin 'Murat arkadaşını gördüğünde, (o) gülüyordu' cümlesinde o zamiri Murat'ın mı yoksa arkadaşının mı yerine kullanıldığı anlaşılamaz. Türkçe'nin bir özelliği olarak genellikle o zamiri yazılmayabilir. Ancak yazılmasa bile, gülüyordu ifadesinin kimden bahsettiği açık değildir.
- ***Genel yargılardan kaçının***. Herkesin aşırı bir şekilde destekleme eğiliminde olacağı maddelerin yazılması çok fazla yarar sağlamayacaktır. Örneğin, "Çalışmak başarıyı artırır" gibi.

## Yapı Uygunluğu ve Anlaşılabilirliği Ölçeği

**Yönerge:**

Lütfen her bir maddeyi dikkatlice okuyun ve

1. 'Yapı Uygunluğu Ölçeği' olarak isimlendirilen ilk sütunda, her bir maddenin ölçme amacımıza ne kadar uygun olduğunu puanlayınız.

2. 'İfade Açıklığı' olarak isimlendirilen ikinci sütunda, yukarıda verilen rehbere göre her bir maddeyi puanlayınız. Eğer bir maddenin zayıf olduğu kanısındaysanız, lütfen bunun nedenini en sağ sütunda aşağıdaki kodları kullanarak belirtiniz.

**A** : Okuma Zorluğu
**B** : Madde Uzunluğu
**C** : Jargon Sözcük
**D** : İki Yönlü İfade
**E** : Çift veya Çoklu Olumsuzlama
**F** : Hangi İsmi Nitelediği Belirsiz Zamir

YRU yaklaşımı risk yönetimi, yönetişim ve uygunluk yönetiminin bir arada düşünülmesi ve uygulamaların teknolojiyle desteklenmesi gerektiğini savunan bir kavramdır. Pek tabi ki, YRU yaklaşımı bileşenlerin bütünleştirilmesini savunsa da, ölçek maddeleri özellikle bir tek bileşeni ölçmeye yönelik olarak hazırlanmıştır. 1-21 arası ölçek maddeleri risk yönetimi, 22-50 arası maddeler yönetişim, 51-69 arası maddeler uygunluk yönetimi ve 70-91 arası maddeler teknoloji konusunda iç denetçinin sorumluluklarını ortaya çıkarmayı amaçlamaktadır.

| Yönetişim | Yapı Uygunluğu Ölçeği | | | İfade Açıklığı (Anlaşılabilirlik) | | | İfade Açıklığına İlişkin Problemin Kodu |
|---|---|---|---|---|---|---|---|
| Maddeler **İç Denetim / İç Denetçi** ifadesiyle başlamaktadır. | DÜŞÜK | ORTA | YÜKSEK | ZAYIF | ORTA | GÜÇLÜ | |
| 1. YRU süreçlerinde yönetim sorumluluğunu almaz. | □ | □ | □ | □ | □ | □ | |
| 2. Mali tabloların ve eklerinin bilgilendirici ve şeffaf olmasını sağlayan kontroller geliştirir. | □ | □ | □ | □ | □ | □ | |
| 3. İşletmenin stratejik amaçları ve diğer güvence fonksiyonlarıyla uyumlu bir iç denetim planı geliştirir. | □ | □ | □ | □ | □ | □ | |
| 4. Kontrolleri test ederken yönetimle koordinasyon halinde ilgili bütün taraflar incelenerek kapsam belirler. | □ | □ | □ | □ | □ | □ | |
| 5. YRU faaliyet sonuçlarının ölçülebilir olmasını sağlar. | □ | □ | □ | □ | □ | □ | |
| 6. YRU süreçlerini geliştirmek amacıyla yetkin personel transferi yapılmasını sağlar. | □ | □ | □ | □ | □ | □ | |
| 7. Amaçlara ulaşılması konusunda makul güvence vermek için YRU süreçlerinin bağımsız değerlendirmesini yürütür. | □ | □ | □ | □ | □ | □ | |
| 8. Yönetimin sorumluluklarını yerine getirmesine ilişkin performansını değerlendirir. | □ | □ | □ | □ | □ | □ | |
| 9. Savunmanın üçüncü hattındaki pozisyonu gereği bağımsızlığını korur. | □ | □ | □ | □ | □ | □ | |
| 10. Yönetim kurulunun pay ve menfaat sahiplerine karşı sorumluluklarını yerine getirmesine katkı sağlayan faaliyetler yürütür. | □ | □ | □ | □ | □ | □ | |
| 11. İşletme paydaşlarının haklarının korunması amacıyla güven ortamının geliştirilmesi için çalışır. | □ | □ | □ | □ | □ | □ | |
| 12. İşletmede yönetişimi geliştirecek politika, yordam ve süreçlerin geliştirilmesine destek olur. | □ | □ | □ | □ | □ | □ | |
| 13. İşletmenin paydaşlarına karşı hesap verebilirliğini sağlamak amacıyla etkili iletişimin geliştirmesini sağlar. | □ | □ | □ | □ | □ | □ | |
| 14. YRU'yu desteklemek amacıyla iç kontrol, risk yönetimi, yönetişim, sürdürülebilirlik gibi konularda çerçeve ve rehberleri bilir. | □ | □ | □ | □ | □ | □ | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 15. | Yöneticilerin işletme paydaşlarına karşı şeffaflığını ve hesap verebilirliğini sağlayan mekanizmaları geliştirir. | □ | □ | □ | □ | □ | □ | |
| 16. | Bilgilendirilmesi gereken paydaşlara ilgili, güvenilir ve zamanında bilgi sunulmasını sağlayan çözümler üretir. | □ | □ | □ | □ | □ | □ | |
| 17. | Birim yöneticileri ve üst yönetim arasında etkileşimi geliştirerek YRU çalışmalarını geliştirir. | □ | □ | □ | □ | □ | □ | |
| 18. | Paydaşlara işletmenin muhasebe ve raporlama sisteminin güvenilir çıktılar ürettiğine ilişkin güvence sağlar. | □ | □ | □ | □ | □ | □ | |
| 19. | İşletmeye paydaşlarının genel kurulda oy kullanma haklarını kullanabilmelerini sağlayacak çözümler hakkında yol gösterir. | □ | □ | □ | □ | □ | □ | |
| 20. | Çalışanların performansının ölçülebilmesi amacıyla doğru ölçütlerin belirlenmesinde yönetime rehberlik eder. | □ | □ | □ | □ | □ | □ | |
| 21. | YRU stratejisinin merkezine etkili bir denetim programını koyar. | □ | □ | □ | □ | □ | □ | |
| 22. | Denetim programını geliştirmek amacıyla kilit yöneticiler (CRO, CEO, CCO) ile bilgi paylaşımında bulunur. | □ | □ | □ | □ | □ | □ | |
| 23. | YRU ile ilgili (iç kontrol, uygunluk, risk yönetimi gibi) diğer güvence çalışanlarıyla koordinasyon içinde olur. | □ | □ | □ | □ | □ | □ | |
| 24. | İşletmenin belirli aralıklarla düzenli olarak şeffaf bir finansal raporlama yapmasına inceleme ve tavsiyeleriyle destek olur. | □ | □ | □ | □ | □ | □ | |
| 25. | İçerden öğrenenlerin ticareti gibi her türlü çıkar amaçlı işlemlerin önlenmesi için tedbir alır. | □ | □ | □ | □ | □ | □ | |
| 26. | Yönetim kurulu, üst yönetim ve bağımsız denetim arasında güçlü bir etkileşim kurulmasına destek olur. | □ | □ | □ | □ | □ | □ | |
| 27. | Doğrudan denetim komitesine raporlama yapar. | □ | □ | □ | □ | □ | □ | |
| 28. | Denetlediği faaliyetlerden ve günlük iş süreçlerinden bağımsızdır. | □ | □ | □ | □ | □ | □ | |
| 29. | İşletmenin tüm birimlerinde, şubelerinde ve bağlı işletmelerinde atanmaksızın kendi inisiyatifiyle hareket edebilir. | □ | □ | □ | □ | □ | □ | |

| Risk Yönetimi | Yapı Uygunluğu Ölçeği | | | İfade Açıklığı (Anlaşılabilirlik) | | | İfade Açıklığına İlişkin Problemin Kodu |
|---|---|---|---|---|---|---|---|
| Maddeler **İç Denetim / İç Denetçi** ifadesiyle başlamaktadır. | DÜŞÜK | ORTA | YÜKSEK | ZAYIF | ORTA | GÜÇLÜ | |
| 30. Risk yönetimi süreçlerine güvence sağlar. | □ | □ | □ | □ | □ | □ | |
| 31. Riskin doğru değerlendirildiğine ilişkin güvence sağlar. | □ | □ | □ | □ | □ | □ | |
| 32. Risk yönetimi süreçlerini değerlendirir. | □ | □ | □ | □ | □ | □ | |
| 33. Temel risklerin uygun şekilde raporlanıp raporlanmadığını değerlendirir. | □ | □ | □ | □ | □ | □ | |
| 34. Temel risklerin üst yönetim tarafından yönetilip yönetilmediğini inceler. | □ | □ | □ | □ | □ | □ | |
| 35. Risklerin belirlenmesi ve değerlendirilmesi sürecini kolaylaştırır. | □ | □ | □ | □ | □ | □ | |
| 36. Risklerin tanımlanması ve değerlendirilmesinde üst yönetime rehberlik eder. | □ | □ | □ | □ | □ | □ | |
| 37. Kurumsal risk yönetimi faaliyetlerinde koordinasyonu sağlar. | □ | □ | □ | □ | □ | □ | |
| 38. Riskler hakkında konsolide raporlar hazırlar. | □ | □ | □ | □ | □ | □ | |
| 39. Kurumsal risk yönetimi çerçevesinin devamlılığını ve gelişimini sağlar. | □ | □ | □ | □ | □ | □ | |
| 40. Kurumsal risk yönetimini yaklaşımının benimsenmesini destekler. | □ | □ | □ | □ | □ | □ | |
| 41. Yönetim kurulunun onayına sunmak için kurumsal risk yönetimi stratejisini geliştirir. | □ | □ | □ | □ | □ | □ | |
| 42. İşletmenin risk iştahını ayarlar. | □ | □ | □ | □ | □ | □ | |
| 43. Risk yönetimi süreçlerini düzenler. | □ | □ | □ | □ | □ | □ | |
| 44. Üst yönetimin risk yönetimi çalışmalarında etkinliğini garanti eder. | □ | □ | □ | □ | □ | □ | |
| 45. Risklere karşı uygulanacak eylemleri belirler. | □ | □ | □ | □ | □ | □ | |
| 46. Risklere karşı uygulanacak eylemleri yönetim adına uygular. | □ | □ | □ | □ | □ | □ | |
| 47. İşletmede risk yönetiminin sorumluluğunu üstlenir. | □ | □ | □ | □ | □ | □ | |
| 48. Savunmanın ikinci hattında bulunan risk ve kontrol birimlerinin etkinliğini geliştirir. | □ | □ | □ | □ | □ | □ | |
| 49. İşletmede riskin tartışılması için ortak bir çerçevenin uygulanmasına ve ortak bir dilin kullanılmasına katkı sağlar. | □ | □ | □ | □ | □ | □ | |
| 50. Kurumsal risk yönetimini göz önünde bulunduran bir iç denetim programı hazırlar. | □ | □ | □ | □ | □ | □ | |

| Uygunluk Yönetimi | Yapı Uygunluğu Ölçeği | | | İfade Açıklığı (Anlaşılabilirlik) | | | İfade Açıklığına İlişkin Problemin Kodu |
|---|---|---|---|---|---|---|---|
| Maddeler **İç Denetim / İç Denetçi** ifadesiyle başlamaktadır. | DÜŞÜK | ORTA | YÜKSEK | ZAYIF | ORTA | GÜÇLÜ | |
| 51. Üst yönetime işletme içi ve dışı şikâyet kanallarının geliştirilmesi konusunda yol gösterir. | □ | □ | □ | □ | □ | □ | |
| 52. Yapılması istenen davranışların teşvik edilmesi amacıyla davranış kuralları ve kodlar hazırlar. | □ | □ | □ | □ | □ | □ | |
| 53. Çalışanların yetki alanları içinde hareket etmelerini teşvik eden işletme uygunluk kültürünü geliştirir. | □ | □ | □ | □ | □ | □ | |
| 54. YRU ile ilgili yerel ve uluslararası düzenlemeleri göz önünde bulundurur. | □ | □ | □ | □ | □ | □ | |
| 55. Uygunluk ile ilgili eğitimler ve tavsiyeler verir. | □ | □ | □ | □ | □ | □ | |
| 56. Uygunluk politikalarının geliştirilmesine destek olur. | □ | □ | □ | □ | □ | □ | |
| 57. Uygunluğu şeklen yasa ve düzenlemelerin yerine getirilmesinden daha fazlası olarak görür. | □ | □ | □ | □ | □ | □ | |
| 58. İşletme kültürünün ve ilgili tüm bireylerin uygunluk amaçlarını destekleyip desteklemediğini değerlendirir. | □ | □ | □ | □ | □ | □ | |
| 59. İşletme stratejilerinin yasa, düzenleme, politika ve yordamlara aykırı özellikler taşımaması konusunda tavsiyeler sunar. | □ | □ | □ | □ | □ | □ | |
| 60. İşletmenin yasa ve düzenlemeler kaynaklı gerekliliklerini izlemek için sistemler kurulmasını sağlar. | □ | □ | □ | □ | □ | □ | |
| 61. İşletme faaliyetleri ile ilgili düzenli olarak uygunluk risk değerlendirmesi yapar ve uygunluk programını gözden geçirir. | □ | □ | □ | □ | □ | □ | |
| 62. İş süreçlerinin uygunluk amaçlarıyla tutarlı hale getirilmesine rehberlik eder. | □ | □ | □ | □ | □ | □ | |
| 63. Hem ulusal hem uluslararası güncel düzenlemelerin takip edilmesini ve hazırlanmasını kolaylaştıran kontrol yordamları geliştirir. | □ | □ | □ | □ | □ | □ | |
| 64. Farklı operasyonel, finansal ve ticari riskler ile karşılaşan işletme birimleri için ayrıntılı uygunluk rehberleri ve yordamlar tasarlar. | □ | □ | □ | □ | □ | □ | |
| 65. Denetim programında işletme politikaları, yordamlar, yasalar ve düzenlemelere uygunluğu test eden incelemelere yer verir. | □ | □ | □ | □ | □ | □ | |
| 66. İşletmenin farklı birimleri arasında uygunluk programlarının tutarlılığı ve bütünleştirilmesi için çaba gösterir. | □ | □ | □ | □ | □ | □ | |
| 67. İşletme çalışanları tarafından uyulması istenen işletme politikalarından kaynaklanan kodları ve kuralları bilir. | □ | □ | □ | □ | □ | □ | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 68. İşletmenin faaliyet alanıyla ilgili zorunlu veya gönüllü sektöre özgü yasal düzenlemeleri bilir. | □ | □ | □ | □ | □ | □ | |
| 69. İşletmenin zorunlu ve gönüllü sınırlarını aşmadan faaliyetini sürdürmesi için gereken incelemeleri yapar. | □ | □ | □ | □ | □ | □ | |

| Teknoloji | Yapı Uygunluğu Ölçeği | | | İfade Açıklığı (Anlaşılabilirlik) | | | İfade Açıklığına İlişkin Problemin Kodu |
|---|---|---|---|---|---|---|---|
| Maddeler **İç Denetim / İç Denetçi** ifadesiyle başlamaktadır. | DÜŞÜK | ORTA | YÜKSEK | ZAYIF | ORTA | GÜÇLÜ | |
| 70. YRU yazılımları üzerinde etkin kontrollerin oluşturulmasına danışmalık yapar. | □ | □ | □ | □ | □ | □ | |
| 71. YRU yazılımlarının tasarımını ve işleyişini düzenli olarak gözden geçirmelidir. | □ | □ | □ | □ | □ | □ | |
| 72. YRU uygulama sürecinde birbirini tekrar eden gereksiz faaliyetlerin belirlenmesini sağlar. | □ | □ | □ | □ | □ | □ | |
| 73. YRU uygulamasının bir parçası olarak teknoloji yazılımlarına ilişkin işletmenin ihtiyaç duyduğu bilgiye sahiptir. | □ | □ | □ | □ | □ | □ | |
| 74. Uygunluk faaliyetlerinin merkezileştirilmesi ve yönetilmesini kolaylaştıran teknolojik çözümler konusunda danışmanlık yapar. | □ | □ | □ | □ | □ | □ | |
| 75. İç kontrol ortamının BT ortamında yürütülmesi için BT uzmanlarını gerektiği gibi yönlendirebilecek seviyede yazılım bilgisine sahiptir. | □ | □ | □ | □ | □ | □ | |
| 76. YRU yaklaşımı doğrultusunda birden fazla amaca hizmet eden kontroller geliştirmeye çalışır. | □ | □ | □ | □ | □ | □ | |
| 77. YRU yaklaşımının uygulamaya geçirilmesi için değişimi anlayacak ve işletme içinde uygulanmasını sağlayacak yöneticilik yeteneğine sahiptir. | □ | □ | □ | □ | □ | □ | |
| 78. YRU'da istenilen etkilere ulaşılması için proaktif bir şekilde çalışır. | □ | □ | □ | □ | □ | □ | |
| 79. BT ile desteklenen denetimler yoluyla hissedar değeri, üretkenlik, şeffaflık ve karar almanın geliştirilmesi yönünde çaba gösterir. | □ | □ | □ | □ | □ | □ | |
| 80. YRU yazılımının seçimi ve işletmeye adaptasyonu sürecinde üst yönetime rehberlik eder. | □ | □ | □ | □ | □ | □ | |
| 81. YRU teknolojisinin uygulanmasında özenli ve bilinçli bir yaklaşımın geliştirilmesi için BT yöneticileriyle işbirliği yapar. | □ | □ | □ | □ | □ | □ | |
| 82. CIO ve CISO ile birlikte risk ve kontrol gerekliliklerini BT ile desteklemek amacıyla işletme çapında teknoloji vizyonu | □ | □ | □ | □ | □ | □ | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ve altyapısını belirlemek için ortak çalışmalar yürütür. | | | | | | | |
| 83. | Gerçek zamanlı risk yönetimini sağlamak için dijital işletme, büyük veri ve bulut teknolojilerin etkisini keşfeder. | □ | □ | □ | □ | □ | □ | |
| 84. | CIO ve CISO ile birlikte kontrol tasarımı ve test programlarıyla desteklenen YRU süreçleri için işletme gerekliliklerinin bilgi teknolojileri ortamında yürütülmesine olanak tanıyan sistem ve uygulamalara uyum sağlamak, işbirliğini geliştirmek ve YRU teknoloji platformunu kurmak için bir plan geliştirir. | □ | □ | □ | □ | □ | □ | |
| 85. | İşletmenin YRU faaliyetlerinin elektronik ortama taşınması konusunda yol gösterir. | □ | □ | □ | □ | □ | □ | |
| 86. | YRU uygulama süreci boyunca üst yönetim ve çalışanlara rehberlik eder. | □ | □ | □ | □ | □ | □ | |
| 87. | İşletmede sürekli denetim için otomatik kontrol modellerinin uygulanmasına destek olur. | □ | □ | □ | □ | □ | □ | |
| 88. | YRU yaklaşımının ihtiyaç duyduğu bilgi güvenliğinin ve bilgi iletişiminin geliştirilmesi sürecinde gerekli teknoloji kaynaklarının kullanılması konusunda çalışmalar yapar. | □ | □ | □ | □ | □ | □ | |
| 89. | İşletme politikası gerekliliklerine dayalı görevleri oluşturmak, onaylamak, korumak, depolamak, izlemek ve otomatikleştirmek için ihtiyaç duyulan teknolojik araçların geliştirilmesini destekler. | □ | □ | □ | □ | □ | □ | |
| 90. | YRU uygulama sürecinde bütünleştirilecek alanlarının belirlenmesine katkı sağlar. | □ | □ | □ | □ | □ | □ | |
| 91. | Sürekli izleme ve sürekli denetimi geliştirmek için işletmenin gerekli teknolojik altyapıya sahip olmasını sağlar. | □ | □ | □ | □ | □ | □ | |

| YRU'nun İşletmeye Faydaları | Yapı Uygunluğu Ölçeği | | | İfade Açıklığı (Anlaşılabilirlik) | | | İfade Açıklığına İlişkin Problemin Kodu |
|---|---|---|---|---|---|---|---|
| **YRU Yaklaşımının İşletme Faaliyetlerine Etkisi** | DÜŞÜK | ORTA | YÜKSEK | ZAYIF | ORTA | GÜÇLÜ | |
| 1. YRU yaklaşımı yönetişim, risk ve uygunluk süreçlerinde bilginin kalitesini artırır. | □ | □ | □ | □ | □ | □ | |
| 2. YRU yaklaşımı riske maruz kalma potansiyeli yüksek işletmelere daha fazla katma değer sağlar. | □ | □ | □ | □ | □ | □ | |
| 3. Bütünleşik risk yönetimi yaklaşımı, işletme faaliyetlerinin kalitesini artırır. | □ | □ | □ | □ | □ | □ | |
| 4. YRU yaklaşımının beklenen faydası maliyetinden fazladır. | □ | □ | □ | □ | □ | □ | |
| 5. Birbirinden kopuk faaliyetler eylemlerin karmaşıklığını artırır, dolayısıyla önemli boşluklara ve gereksiz tekrarlara neden olur. | □ | □ | □ | □ | □ | □ | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 6. | Bütünleşik yaklaşım merkezi bir bakış açısını yansıtır ancak hesap verebilirlik uygun örgütsel seviyelere dağıtılır. | □ | □ | □ | □ | □ | □ | |
| 7. | YRU yaklaşımıyla geliştirilen kontroller yönetişim, risk ve uygunluk süreçlerinde bilginin kalitesini arttırır. | □ | □ | □ | □ | □ | □ | |
| 8. | YRU yaklaşımıyla geliştirilen kontroller riske maruz kalma potansiyeli yüksek işletmelerde daha fazla katma değer yaratır. | □ | □ | □ | □ | □ | □ | |
| 9. | YRU yaklaşımıyla geliştirilen iç kontroller çalışanlar tarafından yürütülen YRU faaliyetlerinin kalitesini manuel kontrollere göre daha fazla arttırır. | □ | □ | □ | □ | □ | □ | |
| 10. | YRU yaklaşımıyla geliştirilen iç kontrollerin faydaları maliyetinden fazladır. | □ | □ | □ | □ | □ | □ | |
| 11. | YRU risk yönetimini işletmeye değer katan bir faaliyete dönüştürür. | □ | □ | □ | □ | □ | □ | |
| 12. | YRU işletmeyi risklere karşı daha esnek bir hale dönüştürür. | □ | □ | □ | □ | □ | □ | |
| 13. | YRU işletmenin risklere ve fırsatlara zamanında karşılık verebilmesini sağlar. | □ | □ | □ | □ | □ | □ | |
| 14. | YRU yaklaşımı yasa ve düzenlemelerin dayattığı zorunluluklara uyum sağlamayı kolaylaştırır. | □ | □ | □ | □ | □ | □ | |
| 15. | Bilgi teknolojisi, YRU süreçlerinde anahtar rol oynar. | □ | □ | □ | □ | □ | □ | |
| 16. | YRU paydaşların beklentilerinin anlaşılmasını ve bunlara öncelik verilmesini sağlar. | □ | □ | □ | □ | □ | □ | |
| 17. | YRU yasal düzenlemelerin, etik standartların, işletmenin taraf olduğu sözleşmelerin ve işletme politikalarının dayattığı sınırları aşmadan işletmenin faaliyetini sürdürmesine destek olur. | □ | □ | □ | □ | □ | □ | |
| 18. | YRU amaçların ve stratejik planlamanın risk bilinciyle oluşturulmasını sağlar. | □ | □ | □ | □ | □ | □ | |
| 19. | YRU örgüt kültürünün yaygınlaştırılmasına katkı sağlar. | □ | □ | □ | □ | □ | □ | |
| 20. | YRU olumsuzluklara ve sürprizlere karşı işletmeyi korur. | □ | □ | □ | □ | □ | □ | |
| 21. | YRU özellikle zorlayıcı şartlarla karşılaşıldığında yapılması istenen davranışları teşvik eder. | □ | □ | □ | □ | □ | □ | |
| 22. | YRU ortak dil, ortak süreçler, ortak teknoloji ve bazı durumlarda ortak çalışanlardan yararlanılmasını sağlayarak iş süreçlerinin maliyetlerini azaltır. | □ | □ | □ | □ | □ | □ | |
| 23. | YRU amaçların açıkça ifade edilmesini sağlayarak, çalışanların motivasyonunu artırır. | □ | □ | □ | □ | □ | □ | |
| 24. | YRU birden fazla amaca hizmet eden etkin kontroller geliştirilmesini kolaylaştırır. | □ | □ | □ | □ | □ | □ | |

**Lütfen aşağıdaki konularla ilgili yorumlarınızı yazınız:**

**1. Madde Sayısı:**
**2. İfadelerin Açıklığı (Anlaşılabilirlik):**
**3. Diğer Konulardaki Yorumlarınız:**

EK-3 İç Denetimin Sorumlulukları Ölçeği Kovaryans Matrisi

| Maddeler | Y3 | Y4 | Y6 | Y7 | Y8 | Y9 | R1 | R2 | R3 | R4 | R6 | R7 | R8 | R9 | R10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Y3 | 0.29 | | | | | | | | | | | | | | |
| Y4 | 0.20 | 0.30 | | | | | | | | | | | | | |
| Y6 | 0.18 | 0.19 | 0.38 | | | | | | | | | | | | |
| Y7 | 0.20 | 0.19 | 0.27 | 0.42 | | | | | | | | | | | |
| Y8 | 0.15 | 0.14 | 0.22 | 0.26 | 0.37 | | | | | | | | | | |
| Y9 | 0.20 | 0.18 | 0.20 | 0.22 | 0.20 | 0.29 | | | | | | | | | |
| R1 | 0.08 | 0.08 | 0.06 | 0.03 | 0.01 | 0.05 | 0.38 | | | | | | | | |
| R2 | 0.06 | 0.07 | 0.06 | 0.06 | 0.02 | 0.05 | 0.25 | 0.38 | | | | | | | |
| R3 | 0.04 | 0.05 | 0.04 | 0.02 | 0.03 | 0.03 | 0.23 | 0.18 | 0.34 | | | | | | |
| R4 | 0.06 | 0.07 | 0.08 | 0.05 | 0.04 | 0.05 | 0.27 | 0.31 | 0.20 | 0.44 | | | | | |
| R6 | 0.01 | 0.03 | 0.03 | 0.01 | 0.01 | 0.01 | 0.20 | 0.17 | 0.23 | 0.17 | 0.35 | | | | |
| R7 | -0.01 | -0.05 | -0.04 | -0.01 | -0.04 | -0.04 | 0.02 | 0.08 | 0.02 | 0.08 | 0.02 | 0.75 | | | |
| R8 | 0.05 | 0.00 | 0.02 | 0.03 | 0.01 | 0.03 | 0.03 | 0.09 | 0.03 | 0.09 | 0.04 | 0.50 | 0.71 | | |
| R9 | 0.00 | 0.01 | 0.01 | 0.02 | 0.00 | 0.00 | 0.03 | 0.07 | 0.04 | 0.09 | 0.03 | 0.48 | 0.50 | 0.81 | |
| R10 | -0.01 | -0.01 | 0.02 | 0.00 | -0.05 | -0.04 | 0.01 | 0.05 | 0.07 | 0.08 | 0.01 | 0.44 | 0.38 | 0.53 | 0.79 |
| R11 | 0.06 | 0.07 | 0.07 | 0.05 | 0.03 | 0.05 | 0.25 | 0.19 | 0.24 | 0.22 | 0.22 | -0.03 | 0.02 | 0.01 | 0.00 |
| R13 | 0.02 | -0.01 | 0.02 | -0.01 | -0.03 | -0.01 | 0.01 | 0.02 | 0.04 | 0.05 | 0.03 | 0.39 | 0.38 | 0.45 | 0.50 |
| U3 | 0.04 | 0.02 | 0.03 | -0.01 | -0.03 | 0.02 | 0.10 | 0.04 | 0.09 | 0.10 | 0.06 | 0.04 | -0.01 | 0.01 | 0.00 |
| U5 | 0.11 | 0.07 | 0.10 | 0.04 | 0.00 | 0.06 | 0.16 | 0.12 | 0.12 | 0.20 | 0.11 | 0.07 | -0.03 | 0.00 | 0.03 |
| U7 | 0.12 | 0.11 | 0.11 | 0.05 | 0.03 | 0.07 | 0.17 | 0.13 | 0.15 | 0.20 | 0.10 | 0.08 | 0.02 | 0.05 | 0.04 |
| U8 | 0.03 | 0.03 | 0.04 | 0.00 | -0.01 | 0.02 | 0.11 | 0.06 | 0.07 | 0.12 | 0.07 | 0.05 | 0.01 | 0.00 | 0.02 |
| U9 | 0.08 | 0.09 | 0.10 | 0.04 | 0.01 | 0.05 | 0.15 | 0.14 | 0.14 | 0.17 | 0.10 | 0.06 | -0.01 | 0.05 | 0.09 |
| U10 | 0.03 | 0.03 | 0.05 | 0.01 | -0.02 | 0.02 | 0.11 | 0.06 | 0.05 | 0.10 | 0.06 | 0.07 | 0.00 | 0.05 | 0.05 |
| U12 | 0.04 | 0.02 | 0.03 | 0.00 | -0.02 | 0.01 | 0.08 | 0.04 | 0.06 | 0.08 | 0.04 | 0.07 | 0.00 | 0.07 | 0.07 |
| BT1 | 0.04 | 0.05 | 0.05 | 0.05 | 0.05 | 0.02 | 0.06 | 0.05 | 0.04 | 0.05 | 0.05 | -0.10 | -0.05 | -0.05 | -0.09 |
| BT2 | 0.02 | 0.04 | 0.04 | 0.06 | 0.03 | 0.02 | 0.08 | 0.08 | 0.08 | 0.11 | 0.07 | -0.08 | -0.06 | -0.03 | -0.05 |
| BT3 | 0.03 | 0.02 | 0.01 | 0.02 | 0.03 | 0.02 | 0.02 | 0.03 | 0.03 | 0.03 | 0.04 | -0.08 | -0.06 | -0.04 | -0.08 |
| BT5 | 0.05 | 0.04 | 0.02 | 0.03 | 0.03 | 0.03 | 0.03 | 0.05 | 0.04 | 0.03 | 0.03 | -0.12 | -0.06 | -0.09 | -0.14 |
| BT6 | 0.07 | 0.08 | 0.06 | 0.06 | 0.06 | 0.03 | 0.06 | 0.09 | 0.05 | 0.08 | 0.06 | -0.10 | -0.06 | -0.04 | -0.08 |
| BT7 | 0.03 | 0.04 | 0.03 | 0.02 | 0.03 | 0.01 | 0.06 | 0.06 | 0.05 | 0.08 | 0.05 | -0.08 | -0.07 | -0.05 | -0.09 |
| BT9 | 0.04 | 0.04 | 0.05 | 0.05 | 0.05 | 0.02 | 0.05 | 0.04 | 0.04 | 0.06 | 0.04 | -0.07 | -0.05 | -0.03 | -0.06 |

İç Denetimin Sorumlulukları Ölçeği Kovaryans Matrisi (Devamı)

| Maddeler | R11 | R13 | U3 | U5 | U7 | U8 | U9 | U10 | U12 | BT1 | BT2 | BT3 | BT5 | BT6 | BT7 | BT9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R11 | 0.36 | | | | | | | | | | | | | | | |
| R13 | 0.02 | 0.76 | | | | | | | | | | | | | | |
| U3 | 0.13 | -0.01 | 0.47 | | | | | | | | | | | | | |
| U5 | 0.16 | 0.02 | 0.39 | 0.75 | | | | | | | | | | | | |
| U7 | 0.18 | 0.02 | 0.41 | 0.65 | 0.8 | | | | | | | | | | | |
| U8 | 0.10 | -0.03 | 0.31 | 0.35 | 0.33 | 0.44 | | | | | | | | | | |
| U9 | 0.15 | 0.02 | 0.32 | 0.47 | 0.52 | 0.32 | 0.65 | | | | | | | | | |
| U10 | 0.08 | -0.01 | 0.29 | 0.32 | 0.3 | 0.36 | 0.32 | 0.49 | | | | | | | | |
| U12 | 0.05 | 0.03 | 0.27 | 0.34 | 0.32 | 0.33 | 0.32 | 0.34 | 0.48 | | | | | | | |
| BT1 | 0.08 | -0.05 | 0.09 | 0.08 | 0.12 | 0.06 | 0.09 | 0.04 | 0.05 | 0.39 | | | | | | |
| BT2 | 0.11 | -0.06 | 0.06 | 0.10 | 0.11 | 0.04 | 0.11 | 0.04 | 0.04 | 0.25 | 0.4 | | | | | |
| BT3 | 0.02 | -0.07 | 0.02 | 0.03 | 0.06 | -0.02 | 0.01 | -0.03 | -0.02 | 0.19 | 0.21 | 0.36 | | | | |
| BT5 | 0.05 | -0.07 | 0.06 | 0.09 | 0.11 | 0.02 | 0.05 | -0.01 | 0.01 | 0.27 | 0.24 | 0.26 | 0.41 | | | |
| BT6 | 0.07 | -0.06 | 0.05 | 0.09 | 0.12 | 0.01 | 0.06 | 0.00 | -0.02 | 0.23 | 0.22 | 0.25 | 0.27 | 0.39 | | |
| BT7 | 0.08 | -0.10 | 0.07 | 0.09 | 0.13 | 0.05 | 0.06 | 0.03 | 0.03 | 0.2 | 0.24 | 0.23 | 0.22 | 0.28 | 0.4 | |
| BT9 | 0.07 | -0.05 | 0.07 | 0.07 | 0.11 | 0.04 | 0.06 | 0.00 | 0.01 | 0.22 | 0.21 | 0.24 | 0.25 | 0.28 | 0.28 | 0.37 |

EK-4 YRU Yaklaşımının Faydaları Ölçeği Kovaryans Matrisi

| Maddeler | YRU1 | YRU6 | YRU7 | YRU8 | YRU9 | YRU10 | YRU11 | YRU12 |
|---|---|---|---|---|---|---|---|---|
| YRU1 | 0.51 | | | | | | | |
| YRU6 | 0.28 | 0.42 | | | | | | |
| YRU7 | 0.29 | 0.32 | 0.43 | | | | | |
| YRU8 | 0.29 | 0.24 | 0.26 | 0.36 | | | | |
| YRU9 | 0.36 | 0.32 | 0.37 | 0.29 | 0.65 | | | |
| YRU10 | 0.33 | 0.31 | 0.36 | 0.27 | 0.44 | 0.54 | | |
| YRU11 | 0.34 | 0.3 | 0.34 | 0.29 | 0.39 | 0.38 | 0.45 | |
| YRU12 | 0.39 | 0.33 | 0.37 | 0.3 | 0.52 | 0.48 | 0.42 | 0.63 |