TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME
ANABİLİM DALI

İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN KAVRAMSAL ANALİZİ

Yüksek Lisans Tezi

Caner ERŞAN

Ankara-2018

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME
ANABİLİM DALI

İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN KAVRAMSAL ANALİZİ

Yüksek Lisans Tezi

Caner ERŞAN

Tez Danışmanı
Yrd. Doç. Dr. Özgür ATEŞ

Ankara-2018

TEZ ONAY SAYFASI

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME
ANABİLİM DALI

Caner Erşan

İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN KAVRAMSAL ANALİZİ

Yüksek Lisans Tezi

Tez Danışmanı : Yrd. Doç. Dr. Özgür ATEŞ

Tez Jürisi Üyeleri

Adı Soyadı	**İmzası**
Yrd. Doç. Dr. Özgür ATEŞ	.....
Prof. Dr. Dilber Uzar	.....
Yrd. Doç. Dr. Hatice Çolpan	.....
.....	.....
.....	.....

Tez Sınavı Tarihi... 15/02/2018

Tez Doğruluk Beyanı Belgesidir.

T.C.
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Yrd. Doç. Dr. Özgür ATEŞ danışmanlığında hazırladığım " İç Denetim Alanında Risk Yönetiminin Kavramsal Analizi (Ankara.2018) " adlı yüksek lisans ☒- doktora/bütünleşik doktora ☐ tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Tarih: 23/02/2018
Adı-Soyadı ve İmza
Caner Erşan

ÖNSÖZ

Tez çalışmamda yardımlarını esirgemeyen, çalışmamın her aşamasında yol gösteren, danışman hocam: Yrd. Doç. Dr. Özgür ATEŞ'e, yüksek lisans programı boyunca her konuda desteğini aldığım Prof. Dr. Orhan ÇELİK'e teşekkür ederim.

Eğitim hayatım boyunca hiçbir fedakârlıktan kaçınmadan beni yetiştiren annem Muhterem ERŞAN, babam Kazim ERŞAN'a, çalışmama katkı sağlayan kız kardeşime, eşim ve canım kızım Zeynep Merve'ye sevgilerimle…

Caner ERŞAN

İÇİNDEKİLER

ÖNSÖZ…….....…….....i
İÇİNDEKİLER.……ii
ŞEKİL ve TABLO LİSTESİ.....v
KISALTMALAR ve SİMGELER.....vi
GİRİŞ…….....1

BİRİNCİ BÖLÜM
İÇ DENETİM

1.1. Uluslararası İç Denetçiler Enstitüsü ve İç Denetimin Tanımı……....4
1.2. İç Denetimin Amacı ve Kapsamı……....6
1.3. İç Denetime İhtiyaç Duyulmasının Nedenleri……....7
1.4. İç Denetimin Fonksiyonları…….....8
1.5. İç Denetimin Katma Değeri……....9
1.6. İç Denetim Uluslararası Mesleki Uygulama Çerçevesi……11
1.6.1. İç Denetimin Misyonu.……...12
1.6.2. Zorunlu Rehber……...13
1.6.3. Tavsiye Edilen Rehber.……...15
1.7. Uluslarası Mesleki Uygulama Çerçevesinde İşin Niteliği Standardı……....15

İKİNCİ BÖLÜM
KURUMSAL YÖNETİM VE İÇ KONTROL

2.1. Kurumsal Yönetimin Tanımı ve Amacı……...20
2.2. Kurumsal Yönetimin Temel İlkeleri…….21
2.3. Kontrol, İç Kontrol ve İç Kontrol Sisteminin Tanımı……..22
2.4. İç Kontrol ve İç Kontrol Sisteminin Amacı ve Önemi.……24
2.5. COSO Komitesi ve COSO İç Kontrol Modeli…….25
2.5.1. COSO İç Kontrol Modeli Bileşenleri.……...…….....27
2.5.1.1. Kontrol Ortamı…….27
2.5.1.2. Risk Değerlendirme…….....28

2.5.1.3. Kontrol Faaliyetleri……...29
2.5.1.4. Bilgi ve İletişim……30
2.5.1.5. İzleme……...30

ÜÇÜNCÜ BÖLÜM
RİSK VE RİSK YÖNETİMİ

3.1. Risk Tanımı……..32
3.2. Risk Çeşitleri ……...32
3.3. Risk Yönetiminin Tanımı ve Amacı…….33
3.4. Risk Yönetiminin Kapsamı…….35
3.5. Risk Yönetim Modelleri……...36
3.5.1. Geleneksel Risk Yönetimi……..37
3.5.2. Gelişmiş (Finansal) Risk Yönetimi…….....38
3.5.3. Stratejik Risk Yönetimi……..39

DÖRDÜNCÜ BÖLÜM
KURUMSAL RİSK YÖNETİMİ

4.1. Kurumsal Risk Yönetiminin Tanımı ve Amacı……40
4.2. Risk İştahı ve Risk Toleransı ……...42
4.3. Kurumsal Risk Yönetiminde Rol ve Sorumluluklar…….44
4.4. COSO Kurumsal Risk Yönetimi Modeli……..46
4.4.1. COSO Kurumsal Risk Yönetimi Modeli Bileşenleri…….48
4.4.1.1. İç Ortam…….....48
4.4.1.2. Hedef Belirleme……49
4.4.1.3. Olay Tanımlama ……..49
4.4.1.4. Risk Değerlendirme……..50
4.4.1.5. Risk Tepkisi……..50
4.4.1.6. Kontrol Faaliyetleri……...51
4.4.1.7. Bilgi ve İletişim.……...51
4.4.1.8. İzleme……...52
4.5. COSO KRY Riskin Strateji ve Performansla Uyumlaştırılması Modeli …… 52

BEŞİNCİ BÖLÜM

RİSKLERİN YÖNETİLMESİ VE KONTROLÜNDE KAVRAMSAL İLİŞKİLER

5.1. Risk Yönetimi, Risk Değerlendirme ve Risk Analizi İlişkisi……...57

5.2. Risk Yönetimi ve Risklerin Kontrolü……...60

5.2.1. Risk ve Kontrol İlişkisi……...61

5.2.2. Risk Yönetimi/Kurumsal Risk Yönetimi ve İç Kontrol İlişkisi…….62

5.2.3. Risk Yönetimi ve Kontrolünde Üç Savunma Hattı……65

5.3. COSO Kurumsal Risk Yönetimi Modeli ve COSO İç Kontrol Modeli İlişkisi…..68

5.4. Risk Yönetimi/Kurumsal Risk Yönetimi ve İç Denetim İlişkisi……..74

ALTINCI BÖLÜM

İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN GİRİFT İLİŞKİLERİNİ GÖSTEREN BİR MODEL ÖNERİSİ VE TARTIŞMALAR

6.1. Öneri 1: Risk Yönetimi ve Kurumsal Risk Yönetimi Arasındaki Kavramsal Farklılıklar….....80

6.2. Öneri 2: Üç Savunma Hattı, İç Denetim, Kurumsal Yönetim, Kurumsal Risk Yönetimi, İç Kontrol, Hedef ve Risk Kavramları Arasındaki İlişkiler……81

6.3. Öneri 3: Kurumsal Risk Yönetimi/Risk Yönetimi ve İç Kontrol Kavramları Arasındaki İlişkiler…….....83

6.4. Öneri 4: Risk Yönetimi ve Risklerin Yönetimi Arasındaki Kavramsal Farklılıklar.85

6.5. Öneri 5: COSO İç Kontrol ve COSO ERM 2004 Modellerinde, Risk Değerlendirme ve Kontrol Faaliyetleri Bileşenleri Arasındaki İlişkiler……86

6.6. Öneri 6: COSO İç Kontrol ve COSO ERM 2004 Modellerinde Hedef Kavramları Arasındaki Farklılıklar…….88

SONUÇ …….90

KAYNAKÇA……..92

GENEL BİLGİLER……...103

ÖZET……103

GENERAL KNOWLEDGE……..104

ABSTRACT…….104

ŞEKİL LİSTESİ

Şekil 1. İç Denetimin Paydaşlar İçin Değeri……..10
Şekil 2. Uluslararası Mesleki Uygulama Çerçevesi……..12
Şekil 3. COSO İç Kontrol Çerçevesi…….27
Şekil 4. Risk Değerlendirme ve Risklere Yanıt Verme Süreci……..29
Şekil 5. Risk Yönetim Süreci…….35
Şekil 6. Geleneksel Risk Yönetim Süreci……..38
Şekil 7. Kurumsal Risk Yönetim Süreci……42
Şekil 8. COSO Kurumsal Risk Yönetimi Çerçevesi……..47
Şekil 9. COSO KRY Riskin Strateji ve Performansla Uyumlaştırılması Modeli……..53
Şekil 10. ISO 31000 Risk Yönetim Süreci…….58
Şekil 11. Risk Yönetimi İçerisinde Kontrollerin Yeri…….61
Şekil 12. Risk Yönetiminde Üç Savunma Hattı……66
Şekil 13. İç Denetimin Kurumsal Risk Yönetimindeki Rolü……76
Şekil 14. İD Alanında RY'nin Girift İlişkilerini Gösteren Bir Model Önerisi ……..79

TABLO LİSTESİ

Tablo 1. Risk Yönetim Modelleri……37

KISALTMALAR

a.g.e. : Adı Geçen Eser

a.g.m. : Adı Geçen Makale

ABD : Amerika Birleşik Devletleri

bkz. : Bakınız

C. : Cilt

CEO : Chief Executive Officer
(İcra Kurulu Başkanı)

COBIT : Control Objectives for Information Technology and Related Technologies
(Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)

COSO : The Committee of Sponsoring Organizations of Treadway Commission
(Treadway Komisyonu'nun Sponsor Kurumlar Kurulu)

COSO ERM: COSO Enterprise Risk Management Integrated Framework
(COSO Kurumsal Risk Yönetimi Bütünleşik Çerçeve)

Çev. : Çeviri

ERM : Enterprise Risk Management
(Kurumsal Risk Yönetimi)

IIA : The Institute of Internal Auditors
(Uluslararası İç Denetçiler Enstitüsü)

IPPF : International Professional Practice Framework
(Uluslararası Mesleki Uygulama Çerçevesi)

ISO : (International Organization for Standardization)
(Uluslararası Standartlar Teşkilatı)

IS0 31000 : ISO 31000 Risk Management
(ISO 31000 Risk Yönetimi Standardı)

İD : İç Denetim

İDF : İç Denetim Faaliyeti

İDB : İç Denetim Birimi

İDKK : İç Denetim Koordinasyon Kurulu

İDY : İç Denetim Yöneticisi

İK : İç Kontrol

İKS : İç Kontrol Sistemi

KRY : Kurumsal Risk Yönetimi

KY : Kurumsal Yönetim

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

Örn : Örnek

RY : Risk Yönetimi

S. : Sayfa

s. : Sayı

T.C. : Türkiye Cumhuriyeti

TİDE : Türkiye İç Denetim Enstitüsü

UİDMUS : Uluslararası İç Denetim Mesleki Uygulama Standartları

UMUÇ : Uluslararası Mesleki Uygulama Çerçevesi

vd. : ve diğerleri

SİMGELER

① : Kurumsal Yönetim

② : Kurumsal Risk Yönetimi

②a : COSO ERM (2004) Modeli

②b : COSO ERM Riskin Strateji ve Performansla Uyumlaştırılması Modeli

③ : İç Kontrol - COSO İç Kontrol Modeli

④ : İç Denetim

⑤ : Risk Yönetim Süreci

⑥ : COSO İç Kontrol Modeli - Risk Değerlendirme Bileşeni

⑦ : COSO ERM Modeli (2004) - Risk Tepkisi Bileşeni

⑧ : COSO İK VE ERM Modellerinde Risk Yanıtları

⑨ : COSO ERM (2004) - Hedef Belirleme Bileşeni

⑩ : COSO ERM Modellerinde Risk İştahı ve Risk Toleransı

⑪ : COSO ERM (2017) Riskin Strateji ve Performans Hedefleriyle Uyumu

⑫ : Riskin Yönetişimi ve Üç Savunma Hattı

⑬ : Kurumsal Yönetim, Kurumsal Risk Yönetimi, İç Kontrol ve İç Denetim İlişkisi

GİRİŞ

Kurumlarda son yıllarda hileli finansal raporlamalarla birlikte yaşanan iflaslar, iş süreçlerinin karmaşıklaşması; risk yönetim faaliyetlerinde, kurumun tüm risklerini kapsayan ve entegre bir model olan stratejik risk yönetimi anlayışını ortaya çıkarmıştır. Yaşanan bu değişim, işletmelerde risk yönetiminde yeni anlayışları ve kavramları da beraberinde getirmiştir. İç denetim (İD) ve risk yönetiminde hızlı şekilde değişen ve yenilenen kavramsal çerçeveler, risk yönetimi (RY) uygulamalarının kurumdan kuruma farklılık göstermesi, uygulayıcılar tarafından İD alanında RY kavramlarının aralarındaki etkileşimin ve ilişkilerin doğru anlaşılmasını zorlaştırmıştır. RY; risklerin yönetilmesi, risklerin kontrolü, risk değerlendirme, iç kontrol (İK), kurumsal risk yönetimi (KRY) ve kurumsal yönetim (KY) gibi kavramlar hakkında uygulayıcılar arasında bir kafa karışıklığı ve tartışma olduğu görülmektedir. Bu kavramların doğru analiz edilebilmesi için, öncelikle iç denetimin uluslararasında genel kabul görmüş güncel tanımından yola çıkmak gerekir. Uluslararası İç Denetçiler Enstitüsü (IIA) tarafından yapılan iç denetimin tanımında; RY, Kontrol ve KY kavramlarına özellikle vurgulama yapıldığı anlaşılmaktadır. Birbirleriyle sıkı ilişki içinde olan bu kavramlar; iç denetim alanında risk yönetiminin doğru anlaşılması ve içselleştirilmesi açısından son derece önemlidir.

Bu çalışmada iç denetim alanında risk yönetimi kavramlarının daha iyi anlaşılması için birinci bölümde; iç denetimin tanımı ve fonksiyonel görevleri incelenmiş, IIA tarafından yayınlanan Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ) açıklanarak, bu çerçevede yer alan, iç denetim faaliyetinin; KY, RY ve kontrol süreçlerini değerlendirmesi ile ilgili bazı bilgilere yer verilmiştir.

İkinci bölümde; KY ve İK kavramları incelenerek, iç kontrolün dünya genelinde kabul görmüş en iyi uygulama modellerinden biri olan ve ‘‘The Committee of Sponsoring Organizations of Treadway Commission - Treadway Komisyonu’nun Sponsor Kurumlar Kurulu’’ (COSO) tarafından 2013 yılında yayınlanan “İç Kontrol Bütünleşik Çerçevesi’’ açıklanmıştır. Üçüncü bölümde; risk ve RY kavramları, RY’nin amacı ve kapsamı, geçmişten günümüze uygulanan RY modelleri anlatılmıştır.

Dördüncü bölümde; KRY’nin tanımı ve amacı, kurumsal risk yönetiminde kullanılan temel kavramlar ile rol ve sorumluluklar açıklanmıştır. 2004 yılında COSO tarafından yayınlanan ve KRY modeli olarak işletmelerde yaygın olarak kullanılan ‘‘COSO Kurumsal Risk Yönetimi Bütünleşik Çerçevesi’’ ve bu çerçeveden revize edilerek 2017 yılında yine COSO tarafından yayınlanan ‘‘COSO KRY Riskin Strateji ve Performansla Uyumlaştırılması Modeli’’ de bu bölümde ayrıntılı olarak ele alınmıştır. Beşinci bölümde; iç denetimde risk yönetiminin kavramsal incelemesini derinleştirmek amacıyla, ilk dört bölümde anlatılan temel kavramlar arasındaki ilişkiler incelenmiştir. Bu bölümde, özellikle iç denetim alanında risk yönetiminin anlaşılmasında kritik bir role sahip olan ve İK, KRY’nin uygulanmasında işletmelerde en çok tercih edilen “COSO İç Kontrol Bütünleşik Çerçevesi’’ ve “COSO KRY Bütünleşik Çerçevesi’’ arasındaki ilişki ayrıntılı olarak değerlendirilmiştir. Ayrıca (IIA) tarafından önerilen “Üç Savunma Hattı Modeli’’ de anlatılarak risk yönetiminin diğer kavramlar arasındaki konumu belirtilmiştir.

Kavramların tarihsel gelişimleri ve bu kavramların uygulanmasına yönelik farklı ülkelerdeki yasal mevzuatlar, bu çalışmada ayrıntılı olarak işlenmemiş; esas olarak kavramların günümüzde en güncel haliyle kullanımı ve sürekli yenilenen RY ve İD anlayışları dikkate alınmıştır.

Bu çalışmanın temelini:

- ∇ IIA'nın iç denetime yönelik bakış açısı,
- ∇ IIA'nın iç denetim için yaptığı tanımdaki kapsam (Risk Yönetimi, Kontrol, Kurumsal Yönetim),
- ∇ IIA'nın yayınladığı Uluslararası Mesleki Uygulama Çerçevesi,
- ∇ COSO komitesinin yayınladığı çerçeveler ve raporlar oluşturmuştur.

Bu çalışmayla, iç denetimin tanımında yer alan ve önemli bir unsur olan risk yönetiminin işletmelerde uygulayıcılar tarafından doğru anlaşılmasının sağlanması kavramsal ve içerik anlamındaki tartışmaların sonlandırılması hedeflenmiş olup; altıncı bölüm olan son bölümde, iç denetim alanında risk yönetimini ilgilendiren temel kavramlar ve çerçevelerle onlara ait ilişkiler, tek bir öneri model üzerinde gösterilerek, altı adet alt başlık altında öneriler sunularak tartışılmıştır.

BİRİNCİ BÖLÜM

İÇ DENETİM

1.1. Uluslararası İç Denetçiler Enstitüsü ve İç Denetimin Tanımı

1941 yılında kurulan IIA: Lake Mary, Florida, ABD'de global merkezi olan uluslararası bir meslek kuruluşudur. IIA; İD mesleğinin, tanınmış otoritesi, kabul edilen lideri, küresel sesi ve başlıca eğiticisidir. Dünya genelinde IIA, 185.000'den fazla üyeye sahiptir. Genel olarak üyeler; İD, RY, KY, İK, bilgi teknolojisi denetimi, eğitim ve güvenlik konularında çalışmaktadır.[1]

İç denetim mesleğine ilişkin ilk standartlar metni çalışmasının IIA tarafından yapılması; iç denetim mesleğinin doğasını, misyonunu ve uygulamalarını köklü bir şekilde etkilemiş, IIA'yı iç denetim mesleğinin öncüsü ve standart belirleyicisi konumuna getirmiştir.[2]

IIA tarafından 1947 yılından günümüze kadar sürekli güncellenen ve geliştirilen iç denetimin tanımına derin anlamlar yüklenildiği görülmektedir. IIA'nın tanımında İD, RY, İK ve KY kavramları arasında güçlü ilişkiler mevcuttur. İç denetim alanında risk yönetiminin kavramsal yerini ve önemini anlamak için öncelikle iç denetimin global tanımından faydalanmak gerekir. Bu nedenle iç denetimin uluslararası alanda kabul görmüş güncel tanımının bu çalışmada temel alınması, risk yönetiminin diğer kavramlarla kurduğu ilişkiler ağının doğru analiz edilmesine yardımcı olacaktır.

---

[1] Uluslararası İç Denetçiler Enstitüsü (IIA).

[2] Çetin Özbek, **İç Denetim**, TİDE Yayınları, 1. Baskı, Yayın No: 3, İstanbul, 2012, C.1, s. 19.

IIA tarafından yapılan son tanımıyla İD: ‘‘Bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden (bağımsız ve objektif)[3] bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun RY, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur. İç denetimin tanımı, iç denetimin temel amaçlarını, doğasını ve kapsamını tanımlamaktadır.’’[4]

Bu tanımla birlikte iç denetim faaliyeti (İDF)[5]; RY ve KY faaliyetlerini, bu faaliyetlerin sorumluluklarını üstlenmeksizin görev alanına almıştır.[6] (Kontrol faaliyetleri diğerlerinden farklı olarak iç denetimin en eski odak noktalarından biridir)

IIA tarafından geliştirilen UMUÇ ve bu çerçeve içerisinde yer alan Uluslararası İç Denetim Mesleki Uygulama Standartları (UİDMUS) söz konusu iç denetim tanımının unsurlarını açıklamaktadır.[7] Standartları ve etik kuralları içeren çerçeve (UMUÇ), bir bütün halinde iç denetimin yukarıda yer verilen küresel tanımı ile birlikte günümüzdeki İD uygulamalarının temelini oluşturmaktadır.[8]

---

[3] **Bağımsızlık**: İç denetim faaliyetinin, İD sorumluluklarını yansız bir şekilde yerine getirme yeteneğini tehdit eden koşullardan özgür olmasıdır. **Objektiflik**: İç denetçilerin görevlerini, iş sonucunda çıkan ürüne gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri şekilde yapmalarını sağlayan tarafsız bir zihinsel tutumdur. IIA, **Uluslararası İç Denetim Standartları (Standartlar)**, UMUÇ, 2017, TİDE (Çev.), http://www.tide.org.tr/uploads/UMUC-2017-updated.pdf, s. 24-27.

[4] IIA, **Definition of Internal Auditing**, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

[5] **İç Denetim Faaliyeti (İDF)**: Kurumun faaliyetlerini geliştirmek ve bunlara değer katmak için tasarlanan bağımsız, objektif güvence ve danışmanlık hizmeti sağlayan birim, bölüm, danışman ekibi veya diğer uygulamacılardır. İDF kurumun RY, kontrol ve KY süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur. IIA, **Standartlar**, UMUÇ, 2017, s. 26.

[6] Davut Pehlivanlı, **Modern İç Denetim**, Beta Yayınları, 2. Baskı, İstanbul, 2014, s. 8.

[7] Çetin Özbek, 2012, s. 3

[8] a.g.e.

IIA tarafından yayınlanan (tanımlar, standartlar, rehberler, vd.) dökümanların Türkçe çevirileri, Türkiye İç Denetim Enstitüsü (TİDE)[9] tarafından yapılmaktadır.

1.2. İç Denetimin Amacı ve Kapsamı

İDF'nin amacı; kurumun hedeflerine ulaşması, KY hedeflerine ulaşılmasını sağlamak ve iç kontroller hakkında bağımsız ve tarafsız güvence sağlamaktır. Aynı zamanda işletme kültürü, sistemleri ve süreçleri ile ilgili, bilgi ve deneyim sahibi iç denetçiler ile yürütülen İDF; yönetime RY, kontrol ve KY süreçlerinin gelişiminde, bağımsız görüş ve önerileri ile fayda sağlamaktadır.[10]

İç denetimin temel amacı kuruma değer katmaktır. İD kurumların; İK, RY ve KY sistemlerinin geliştirilmesine katkıda bulunmak, iş süreçlerin iyileştirilmesini, kaynakların etkili ve verimli kullanılmasını sağlamak, hata, hile ve su istimallerin önlenmesine yardımcı olmak, risklerin neden olabileceği zararları azaltmak, kurumların itibarını korumak ve hedeflerine ulaşmasına katkı sağlamak amacıyla değer yaratır.[11]

İD, bir kurumun tüm faaliyetlerini kapsamaktadır. İDF risk değerlendirmesini esas alarak; KY, RY ve İK süreçlerinin olası bir risklere karşı, risklerin belirlenmesi, tanımlanması ve bu risklerle mücadele edilmesi konularında ne derece yeterli ve etkin olduğunun belirlenmesini sağlamaktadır.[12]

---

[9] İç denetçilerin meslek örgütü olarak 1995 yılında kurulan TİDE, İD mesleğinin ve profesyonellerinin uluslararası standartlar ile uyumlu, küresel seviyede yetkin uygulamaları için güvence oluşturmaktadır. TİDE, İD uygulamalarında; sertifikasyon, uluslararası standartlar, eğitim, ulusal kongreler, yayıncılık, araştırma, kariyer gelişimi ve rehberlik gibi çok çeşitli hizmetler sunmaktadır. www.tide.org.tr/

[10] TİDE, Kurumsal Yönetimin Güvencesi İç Denetim, **Platin Dergisi**, https://www.tide.org.tr/uploads/news/Platin_Ek.pdf,

[11] Gürdoğan Yurtsever, İç Denetimin Fonksiyonları ve Katma Değeri, **Finans Politik & Ekonomik Yorumlar**, 2015, C.52, S.602, s. 90, http://www.ekonomikyorumlar.com.tr/dergiler/makaleler/602/sayi_602_makale-06.pdf

[12] Deniz Ezgi Günererdem, **Kamu İç Denetimde Kalitenin Sağlanması: İç Denetimde Kalite Güvence Sistemleri**, T.C. Maliye Bakanlığı, Devlet Bütçe Uzmanlığı Araştırma Raporu, Ankara, 2006, s. 17.

İç denetimin birincil amacı, İKS'nin etkinliğinin değerlendirilmesi ve geliştirilmesine yönelik tavsiyelerde bulunmaktır.

''İD'nin tanımı iç denetimin alanını açıkça belirlemiştir. İşletmelerin tüm RY, kontrol ve yönetişim sistemleri, süreçleri, faaliyetleri ve uygulamaları İDF'nin kapsamına dahildir. İDF'nin kapsamı (alanı) kurumdaki fonksiyonel alanlar değil, sistemler bazında tanımlanmıştır. RY, kontrol ve yönetişim süreçleri denilirken alan daraltılmıştır. İD süreç ya da fonksiyon bazlı gerçekleştirilecektir, çünkü işin esas hedefi budur ancak güvence hizmeti RY, kontrol ve yönetişim süreçleri üzerinden yapılacaktır.''[13]

İD'nin kapsamını aşağıdaki gibi özetlemek mümkündür.[14]

- KY süreçlerinin denetimi
- RY süreçlerinin denetimi
- İK sistemlerinin denetimi
- Bilgi teknolojileri
- Danışmanlık faaliyetleri

1.3. İç Denetime İhtiyaç Duyulmasının Nedenleri

Kurumlarda İD; risk ve kontrol değerlendirme faaliyetlerine destek sağlar, işletme faaliyetlerini bağımsız ve objektif bir gözle izler, risk ve kontrol faaliyetleri ile ilgili tavsiyelerde bulunur, kontrollerin uygunluğunu ve etkinliğini ölçer.[15]

[13] Bertan Kaya, **İç Denetime İlişkin Kafa Karıştıran 6 Konu ve Bunlara İlişkin Yorumlar**, 2014.
[14] Ç. Özbek, 2012, s. 20.
[15] Ali Kamil Uzun, **İç Denetim Nedir**, Deloitte Türkiye, http://www.denetimnet.net/UserFiles/Documents/Makaleler/%C4%B0%C3%A7%20Denetim/%C4%B0%C3%A7%20Denetim%20Nedir-Makale.pdf

İD, şirket ve kurumlarda mali raporlama sisteminin güvenilirliği, yasal düzenlemelere uygunluk, faaliyetlerin (ekonomikliği, etkinliği ve verimliliği)[16], bilgi sistemlerinin güvenliği ve güvenilirliği için önemli bir yere sahiptir. İD, şirket ve kurumlarda yönetsel hesap verebilirliğin yerleşmesine çok büyük katkı sağlamaktadır. RY'nin bir parçası olarak önleyici yönü bulunmaktadır. KY kalitesini artırır, kurumsal değeri yükseltir. Paydaşlar ve menfaat sahipleri için güvence sağlar.[17]

İD, yönetsel hesap verebilirliğin kurum kültürüne yerleşmesine katkı sağlar. İD, işletmenin KY uygulamalarına yönelik yaptığı etkinlik ve verimlilik değerlendirmeleri ile yönetimin bilinçlendirilmesi adillik, şeffaflık, hesap verebilirlik ve sorumluluk ilkelerine uygun yönetim uygulamalarının geliştirilmesi ve bu şekilde işletmenin kurumsal devamlılığı ve itibarının arttırılarak, amaçlarının gerçekleştirilmesine yardımcı olur.[18]

1.4. İç Denetimin Fonksiyonları

İD faaliyetinin ana fonksiyonları, güvence ve danışmanlık hizmetleri olarak ikiye ayrılır.

Güvence Hizmetleri: İç denetçinin edindiği mevcut delilleri objektif bir tutumla değerlendirmesi ve süreçler, sistemler hakkında görüş sunması olarak özetlenebilir.

[16] **Ekonomiklik**: Bir faaliyetin planlanmış sonuçlarına ya da çıktılarına ulaşmak için, uygun düzeydeki kaliteyi de gözeterek, kullanılan kaynakların maliyetini en aza indirilmesidir. **Etkinlik**: Kullanılan kaynaklarla, bir faaliyetin sonuçlarını ya da çıktılarını azami düzeye çıkarmayı ifade eder. **Etkililik**: Hedeflere ulaşma derecesiyle ilgili olup, istenilen etki ile gerçekleşen etki ya da bir başka ifadeyle amaçlar ile çıktılar ve sonuçlar arasındaki ilişkiyi ifade eder. **Verimlilik**: Kurum faaliyetlerinde kullanılan girdilerin sabit kalması koşuluyla, belirli bir kalitede en fazla mal veya hizmetin sunumu ya da belirli bir miktar ve kalitedeki mal ve hizmeti sunmak için en az miktarda girdi kullanılmasıdır. İDKK, **Kamu İç Denetim Terimler Sözlüğü**, T.C. Maliye Bakanlığı.

[17] Ali Kamil Uzun, a.g.m.

[18] TİDE, Kurumsal Yönetimin Güvencesi İç Denetim.

Güvence hizmetlerinin nitelik ve kapsamı iç denetçi tarafından bizatihi belirlenir. Güvence hizmetlerinin aşağıda açıklanan şekilde üç tarafı vardır:[19]

(1) Süreç sahibi: Değerlendirilecek sürecin sahibi,

(2) İç denetçi: Değerlendirmeyi yapacak taraf,

(3) Kullanıcı: Değerlendirme sonunda güvence hizmetinden fayda sağlayacak taraf.

Danışmanlık Hizmetleri: Danışmanlık görevleri tavsiye niteliğindedir. Danışmanlık hizmeti almak isteyen müşteri özel olarak talepte bulunur ve hizmet gerçekleştirilir. Niteliği ve kapsamı, değerlendirmeyi talep eden müşteriyle iç denetçi arasındaki anlaşmaya göre şekillenir. Danışmanlık hizmetleri, güvence hizmetlerinden farklı olarak iki tarafa sahiptir:[20]

(1) İç Denetçi: Değerlendirmeyi yapacak taraf

(2) (Görevin Müşterisi)[21]: Danışmanlık hizmetini talep eden taraf

İç denetçiler; KY, RY ve kontrol süreçlerinin geliştirilmesine yönelik tavsiyelerde bulunarak danışmanlık hizmeti verebilirler.

1.5. İç Denetimin Katma Değeri

Kurum içindeki yönetim organları, kurumsal politikalara uygunluğun sağlanması, iç kontrollerin etkin ve etkili çalışıp çalışmadığından emin olmak için güvence almak isterler ve bu konuda en büyük destekçileri iç denetçilerdir. İç denetçiler; kuruma faydalı olacak hangi yolların izlenmesi gerektiği hakkında, derin analiz yeteneği, objektif değerlendirme tutumu ve içgörüye sahiptirler.[22]

---

[19] IIA, **Standartlar**, UMUÇ, 2017, s. 2.

[20] a.g.e.

[21] **Görev (Engagement)**: İD, kontrol öz değerlendirme incelemesi, suiistimal incelemesi veya danışmanlık gibi belirli İD işi, vazifesi veya gözden geçirme faaliyetidir. Bir görev, çok sayıda işten veya belirli amaç-lara ulaşmayı amaçlayan faaliyetlerden oluşabilir. a.g.e, s. 26.

[22] IIA, **İç Denetim Güvence İçgörü Nesnellik**, TİDE (Çev.), https://www.tide.org.tr/uploads/news/IIA_Ic_Denetimin_Paydaslar_Icin_Degeri_Detay.pdf

İç denetimin paydaşlar için değerini gösteren kavramlar aşağıdaki şekilde gösterilmiştir. [23]



Şekil 1: İç Denetimin Paydaşlar İçin Değeri

İç denetimin değer teklifi, İD yoluyla bir kuruma sunulan aşağıdaki üç ana değer (Güvence, anlayış/içgörü, nesnellik/objektiflik) üzerine kuruludur:[24]

Güvence (Yönetişim, Risk ve Kontrol): İD; KY, RY ve kontrol süreçleri için güvence sağlayarak kurumların hedeflerine ulaşmasına yardımcı olur.

Anlayış/İçgörü (Katalizör, Analizler ve Değerlendirmeler): İş süreçlerinin değerlendirilmesi ve veri analizi yoluyla yapılan tavsiyelerle İD, bir kurumun etkinlik ve verimliliğinin geliştirilmesi için bir katalizör görevi görür.

Nesnellik/Objektiflik (Dürüstlük, Hesapverilebilirlik ve Bağımsızlık): Dürüstlük ve hesap verebilirlik ilkelerine bağlı olan İD, yönetim kademeleri için güvenilir bir kaynaktır. Bağımsız bakış açısına sahip İD'ye, yönetim organları ve üst düzey yöneticiler bu özelliğinden dolayı güven duymaktadır.

[23] IIA, **İç Denetimin Paydaşlar İçin Değeri**, TİDE (Çev.), https://www.tide.org.tr/uploads/news/IIA_Ic_Denetimin_Paydaslar_Icin_Degeri.pdf
[24] IIA, **İç Denetimin Katma Değeri ve Kapasite Modeli**, Ek Rehber, 2012, TİDE (Çev.), https://www.tide.org.tr/uploads/SG_Ic_Denetimin_Katma_Degeri.pdf

1.6. İç Denetim Uluslararası Mesleki Uygulama Çerçevesi

UMUÇ, International Professional Practices Framework (IPPF), iç denetim uygulamalarına ilişkin küresel çapta İD mesleğinin uygulama kurallarını belirleyen en temel rehberi oluşturmakta aynı zamanda IIA'yı iç denetim mesleğine ilişkin saygın, uluslararası alanda kabul görmüş, kural koyucu bir konuma getirmektedir.[25]

UMUÇ, IIA'nın küresel anlamda otoritesini tesis etmesinde ve standartları belirlemesindeki pozisyonunu güçlendirmesinde önemli rol oynamaktadır. UMUÇ'un hayata geçirilmesi, İDF'nin sorumluluk üstlendiği farklı ortamlara göre değişiklik gösterir. İD faaliyetleri dünya genelinde farklı ülkelerde ve farklı ortamlarda icra edilmektedir.[26]

UMUÇ/IPPF'de bazı değişiklikler yapılarak, 2015 yılında yenilenmiştir. UMUÇ, zorunlu rehber ve tavsiye edilen rehber olarak ikiye ayrılmıştır. İç denetimin misyonu tanımlanmış ve temel prensipler eklenmiştir. Uygulama önerileri de uygulama rehberlerine dönüştürülmüştür. Yenilenen UMUÇ; misyon, zorunlu rehber ve tavsiye edilen rehber olarak üç kısımdan oluşmakta olup, misyon diğerlerinden farklı olarak tüm çerçeveye entegre edilmiştir.

[25] Ç. Özbek, 2012, s. 29.
[26] IIA, **UMUÇ**, TİDE (Çev.), https://www.tide.org.tr/page.aspx?nm=umuc

Yenilenen UMUÇ aşağıdaki şekilde gösterilmiştir.[27]



Şekil 2: Uluslararası Mesleki Uygulama Çerçevesi

1.6.1. İç Denetimin Misyonu

‘‘IIA’nın tanımına göre İD’nin misyonu: Risk bazlı, objektif güvence sağlayarak ve tavsiye ile öngörülerle organizasyonel değeri korumak ve geliştirmektir. İç denetimin misyonu, iç denetimin kurumun içerisinde gerçekleştirmeyi hedeflediği şeyleri ifade eder. Misyonun yeni UMUÇ’da ki yeri özel olarak, zorunlu rehber ve tavsiye edilen rehberden farklı bir şekilde konumlandırılmıştır.’’[28]

[27] IIA, **YENİ IPPF**, 2015, TİDE (Çev.), http://www.tide.org.tr/uploads/IPPF-Toolkit-Copy-Flyer-and-Ad%2029072015.pdf
[28] a.g.m.

1.6.2. Zorunlu Rehber

İD mesleki uygulamaları için, zorunlu rehberde öngörülen prensiplere uyulması şarttır. Zorunlu rehber kamunun görüşlerinin alınmasını da içeren bir durum tespiti süreci ile geliştirilmiştir. Yeni UMUÇ'un zorunlu unsurları şunlardır:[29]

- İç Denetimin Tanımı
- Ana Prensipler
- Standartlar
- Etik Kurallar

❒ İç Denetimin Tanımı

IIA'nın tanımına göre: "İD bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İD sistematik ve disiplinli bir yaklaşımla RY, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirir ve gelişimine katkı sağlamak amacıyla tavsiyelerde bulunur.''[30]

❒ Ana Prensipler

Yenilenen UMUÇ'a göre ana prensipler aşağıdaki gibi açıklanmıştır.[31]

- ♦ Dürüst ve faziletli davranır.
- ♦ Yetkinlik ve profesyonel özen sergiler.
- ♦ Objektiftir ve etki altında kalmaz. (Bağımsızdır)
- ♦ Kurumun stratejileri, hedefleri ve riskleri ile uyumludur.
- ♦ Uygun olarak konumlandırılmıştır ve yeterli kaynağa sahiptir.

[29] IIA, **YENİ IPPF**, 2015, TİDE (Çev.).
[30] IIA, **Definition of Internal Auditing**.
[31] IIA, **Ana Prensipler**, UMUÇ, TİDE Çev.), http://www.tide.org.tr/page.aspx?nm=Ana_Prensipler

- Kalite ve sürekli gelişimi esas alır.
- Etkili bir şekilde iletişim kurar.
- Risk bazlı güvence sağlar.
- İçgörülü, proaktif ve gelecek odaklıdır.
- Kurumsal gelişimi teşvik eder.

❒ Standartlar

‘‘Standartlar, nitelik standartları ve performans standartları şeklinde iki gruba ayrılmıştır. Nitelik standartları, iç denetim faaliyetlerini gerçekleştiren kurumların ve kişilerin özelliklerine açıklarken; performans standartları, iç denetimin doğasını açıklamaktadır.’’[32]

(Standartlar)[33] ilke temelli ve uyulması zorunlu durumları açıklamaktadır. Temel zorunluluklara ilişkin ‘‘Beyanlar’’ ve standartlarda geçen terim ve kavramları açıklayan “Yorumlar”dan oluşmaktadır.[34]

❒ Etik Kurallar

İD mesleğinin uygulanması hakkında ‘‘İlkeler’’ ve iç denetçilerden beklenen davranış tarzını tanımlayan ‘‘Davranış Kuralları’’ndan oluşan Etik kurallarının amacı, İD mesleğinin etik kültürünü geliştirmektir. Objektif güvence sağlama amaçlı hareket edecek bir iç denetim mesleği için, etik kurallar oluşturulması önemli bir gereksinimdir. IIA’nın etik kuralları aşağıda belirtilen iki önemli kısımdan oluşmaktadır:[35]

---

[32] IIA, **Standartlarla Tanışma Metni**, TİDE (Çev.), https://www.tide.org.tr/uploads/pdf/StandartlarlaTanismaMetni.pdf

[33] Bu çalışmada İD standartları ayrıntılı olarak açıklanmamış, konu bütünlüğünün dağılmaması ve çalışmanın özüne vurgu yapılması amacıyla performans standartlarında kendine yer bulan, işin niteliği ana başlıklı standartta (RY, KY, İK) ile ilgili konular detaylı olarak incelenmiştir.

[34] IIA, **Standartlar**, UMUÇ, 2017, s. 1.

[35] IIA, **Etik Kurallarıyla Tanışma Metni**, TİDE (Çev.), https://www.tide.org.tr/page.aspx?nm=EtikKurallari#etkurtan

1.6.3. Tavsiye Edilen Rehber

IIA tarafından bir resmi onay süreciyle hazırlanmış ve onaylanmıştır. İç denetimin tanımı, etik kurallar ve standartların ve yeni İD misyonunun etkin uygulanması için gerekli uygulamaları tanımlar. Tavsiye edilen rehber, uygulama ve tamamlayıcı rehberler olarak ikiye ayrılmıştır:[36]

Uygulama Rehberi: ‘‘Geniş kapsamlı bir rehberler seti olan uygulama rehberleri, iç denetçilere standartlara uyumu sağlamak konusunda yardımcı olur.’’

Tamamlayıcı Rehber: ‘‘Ayrıntılı bir rehber seti olan tamamlayıcı rehberler spesifik alanlarda ve uygulamalarda iç denetçilere yardımcı olur.’’

1.7. Uluslararası Mesleki Uygulama Çerçevesinde İşin Niteliği Standardı

İç denetimde yapılacak faaliyetlerin doğasını açıklayan ve performans standartlarında yer alan işin niteliği standardı, İDF’nin esas yapacağı işin niteliğini yani KY, RY ve kontrol süreçlerinin değerlendirilmesinde üstlenmesi gereken vazifeyi detaylı olarak açıklamaktadır.

Standart 2100 İşin Niteliği: ‘‘İDF sistematik, disiplinli ve risk esaslı bir yaklaşımla; KY, RY ve kontrol süreçlerini değerlendirmek ve bu süreçlerin iyileştirilmesine katkıda bulunmak (zorundadır).[37] Denetçiler proaktif olduklarında, yaptıkları değerlendirmelerle yeni anlayışlar sunduğunda ve olası gelecek etkileri göz önünde bulundurduklarında iç denetimin güvenilirliği ve değeri artmaktadır.’’[38]

---

[36] IIA, **YENİ IPFF**, 2015.

[37] IIA, **Standartlar**, UMUÇ, 2017, s. 15-29.

Zorundadır (Must): Standartlarda kayıtsız şartsız bir gerekliliği vurgulamak için zorundadır kelimesi kullanılmıştır.

[38] a.g.e, s. 15.

İç denetimin odak noktası olan KY, RY ve kontrol süreçlerinin değerlendirilmesi, işin niteliği standardı kapsamında değerlendirilmek zorundadır. IIA, UMUÇ çerçevesinde zorunlu kıldığı standartların yanısıra tavsiye edilen rehberde yer alan uygulama önerileri ile de (yeni adı uygulama rehberleriyle) bu süreçlerin değerlendirilmesine kolaylık sağlamaktadır. İşin niteliği standardı; kurumsal yönetim süreçlerinin değerlendirilmesi, RY süreçlerinin değerlendirilmesi ve kontrol süreçlerinin değerlendirilmesi olarak üç alanda gerçekleştirilmektedir.

Kurumsal Yönetim Süreçlerinin Değerlendirilmesi: Kurumun stratejik hedeflerine ulaşması için oluşturduğu organizasyonel yapının yeterliliği, üst düzey yöneticilerin çalışmalarının (yönetim kurulunca)[39] değerlendirilmesini içermektedir. Tüm dünyada özellikle halka açık firmalarda uygulanmak üzere yürürlüğe konulan KY prensipleri, yönetim kurullarının ve alt komitelerinin kurum faaliyetlerinin izlenmesi konusundaki rol ve sorumluluklarını artırarak şeffaflık ve hesap verilebilirliği güçlendirmeye çalışırken aynı zamanda firmaların etkin birer RY ve İK sistemine sahip olmalarını öngörmekte ve bu sistemlerin kurulması ve etkin işletilmesi sorumluluğunu ağırlıklı olarak yönetim kurullarına ve üst düzey yöneticilere vermektedir. Yönetim kurullarının ve üst düzey yöneticilerin bu görevleri yerine getirmede en önemli yardımcıları ise söz konusu sistemlerin işlerlik ve yeterliliğine dair yapacağı bağımsız değerlendirmelerle iç denetim birimleri olmaktadır.[40]

[39] **Kurul (Board)**: Kurumun faaliyetlerini yönetmek ve/veya gözetmekle sorumlu olan ve üst yönetime sorumluluk verebilen en yüksek yönetim organıdır. (Örn: Yönetim Kurulu, idare heyeti veya mütevelli heyeti) Yönetişim düzenlemeleri bölge ve sektörler arasında farklılık gösterse de, genellikle kurul yönetimde olmayan üyelerden oluşur. Eğer böyle bir kurul mevcut değilse, standartlar da yer alan "Kurul" kelimesi kurumun yönetişiminden sorumlu grubu veya kişiyi ifade eder. Ayrıca standartlar da yer alan "Kurul" yönetim organının yetkilerini devrettiği bir komite ya da organa da tekabül edebilir. (Örn: Denetim komitesi), IIA, **Standartlar**, UMUÇ, 2017, s. 27.

[40] Ç. Özbek, 2012, s. 21.

Kurumsal yönetim süreçlerinin değerlendirilmesi, iç denetçiler tarafından aşağıdaki sorulara odaklanarak gerçekleştirilir.[41]

• Kurum içinde etik değerler belirlenmiş mi? ve bu değerler çalışanlara teşvik ediliyor mu?

• Kurumsal yönetim süreçleri, performans ve hesap verebilirlik konularında etkin mi?

• Kurum içerisinde risk ve kontrol hakkındaki bilgiler doğru yerlere iletiliyor mu?

• Yönetim kurulu, iç ve dış denetçiler arasındaki etkin iletişimi ve eşgüdümü tesis edebiliyor mu?

Kurumsal yönetim süreçlerinin değerlendirilmesi genellikle doğrudan KY süreçleri üzerinden bağımsız bir değerlendirme yapmaktan ziyade, risk ve kontrol süreçlerinin değerlendirilmesi ile bütünleştirilerek yapılır. Risk ve kontrol süreçlerine yönelik bir değerlendirme aynı zamanda kurumsal yönetim süreçlerine doğrudan temas edecektir.

Risk Yönetim Süreçlerinin Değerlendirilmesi: RY, kurumun hedeflerine ulaşması gayesiyle makul bir güvence sağlamak amacıyla potansiyel olayların belirlemesi, değerlendirmesi, yönetilmesi ve kontrol edilmesi sürecidir. RY, KY'nin önemli bir unsurudur. RY kurumun diğer operasyonel süreçlerinden ayrı bir süreç olmayıp kurumun günlük faaliyetlerinin içerisinde adapte edilen bütünleyici bir süreçtir. RY formel veya kurallara bağlanmış bir şekilde icra edilebileceği gibi günlük faaliyetlerin izlenmesi sırasında da icra edilebilir. Ancak formel veya kurallara bağlanmış bir RY'nin KY süreçlerine dahil edilmesi RY'nin etkinliğini kuşkusuz artıracaktır. Bunun aksine günlük faaliyetlerinde karşı karşıya olduğu risklerin etkin bir şekilde yönetilmemesi kurumu başarısızlık veya iflas riskliyle yüz yüze getirebilecektir. Risk yönetimi faaliyetlerinin iç denetim faaliyetleri tarafından değerlendirilmesi İDF'nin kapsamının en önemli üç unsurundan birisini oluşturmaktadır.[42]

---

[41] IIA, **Kurumsal Yönetim**, UMUÇ, Uygulama Rehberi 2110, Temmuz 2015, TİDE (Çev.), https://www.tide.org.tr/

[42] Ç. Özbek, 2012, s. 120-121.

RY konusu hem günümüzde hem de yakın gelecekte İDF'nin en önemli kapsamını ve faaliyet alanını oluşturmaya devam edecektir. İDB gerek RY konusunda kurum yönetici ve çalışanlarının bilgilendirilmesi ve gerekse söz konusu sistemlerin yeterliliği ve etkinliğine dair yapacağı bağımsız değerlendirmeler ile kurumun hedeflerinin gerçekleştirilmesine yardımcı olacaktır.[43]

Risk yönetim süreçlerinin değerlendirilmesi, iç denetçiler tarafından aşağıdaki sorulara odaklanarak gerçekleştirilir.[44]

• Organizasyonel hedefler kurumun misyonu ile uyumlu mu?

• Kritik riskler belirlenmiş ve değerlendirmeye alınmış mı?

• Riskleri hafifletmeye yönelik aksiyonlar, risk iştahı ile uyumlu mu?

• İlgili risk bilgileri kurumun genelinde zamanında elde edilip yayınlanabiliyor mu?

Kontrol Süreçlerinin Değerlendirilmesi: Kontrol süreçleri: "Risklerin, kurumun kabul etmeye gönüllü olduğu sınırlar içinde kalmasını sağlamak gayesiyle tasarlanan ve işletilen kontrol çerçevesinin parçası olan faaliyet politika ve prosedürlerdir.''[45]

''İç kontroller riskleri kontrol altında tutmak ve kurumsal hedef ve amaçlara ulaşma ihtimalini arttırmak amacıyla alınan tedbirlerdir. Bu tedbirlerin uygulanabilmesi için kurum içerisinde bazı politika ve prosedürlerin belirlenmesi gerekir. Belirlenen politika ve prosedürler kontrol süreçleri aracılığı ile işleme konulur. Kurum içerisinde bütün çalışanlar iç kontrol konusunda önemli görevlere sahiptir. Kurum içinde gerçekleştirilen kontroller (iç kontroller), bir iç denetçinin çalışmalarında birinci odak noktasıdır. İç denetçiler, kontrol süreçlerinin etkinliğini ve verimliliğini nesnel bakış açılarıyla değerlendirir. İç kontrollerin tasarım ve işlevselliğini inceleyerek yeterli veya uygun olup olmadığına karar verir ve önerilerde bulunur.''[46]

---

[43] a.g.e, s. 21.

[44] IIA, **Risk Yönetimi**, UMUÇ, Uygulama Rehberi 2120, Aralık 2016, TİDE (Çev.), https://www.tide.org.tr/

[45] IIA, **Standartlar**, UMUÇ, 2017, s. 27.

[46] IIA, **İç Denetim Güvence İçgörü ve Nesnellik**, TİDE (Çev.).

Kontrol süreçlerinin değerlendirilmesi, iç denetçiler tarafından aşağıdaki sorulara odaklanarak gerçekleştirilir.[47]

• Kontroller doğru tasarlanmış mı? Tasarlanmış ise faâl çalışıyor mu? Kurumun stratejik hedeflerine ulaşmasına katkı sağlıyor mu?

• Finansal ve operasyonel bilgiler, güvenilir ve doğrumu?

• Faaliyetler etkin ve verimli gerçekleştiriliyor mu?

• Varlıklar korunuyor mu?

• Kanun ve kurum içi yönetmeliklere uyum sağlanıyor mu?

[47] IIA, **Standartlar**, UMUÇ, 2017, s. 15-16.

İKİNCİ BÖLÜM

KURUMSAL YÖNETİM VE İÇ KONTROL

2.1. Kurumsal Yönetimin Tanımı ve Amacı

Türkçeye kurumsal yönetişim veya kurumsal yönetim olarak çevrilen ‘‘Corporate Governance’’ kavramı, kurumlarda son yıllarda popüler bir kavram haline gelmiştir. KY; şirketlerin kârlılığının artırılması, şirket faaliyetlerinin etkin ve verimli çalışması, bu vesile ile hissedarların ekonomik kazançlarının artırılmasını sağlayan kanun, yönetmelik ve gönüllü özel sektör uygulamalarının bileşimidir.[48]

Son yirmi yılda dünya genelinde yaşanan finansal krizler ve (şirket iflasları)[49] KY kavramının ortaya çıkmasında etkili olmuştur. Finansal raporlamalara yönelik duyulan güvensizlik ortamının yeniden dizayn edilmesi amacıyla birçok ülkede KY alanında çeşitli yasa ve yönetmelikler çıkarılmıştır.[50]

Kurumsal Yönetim Süreçleri: Yönetişim standartlarda: ‘‘Kurumun amaçlarını gerçekleştirmeye yönelik olarak faaliyetlerini yönlendirmek, yönetmek, izlemek ve bu faaliyetler hakkında bilgi vermek gayesiyle yönetim kurulunun yerine getirdiği süreçlerin ve yapıların birleşimi’’ şeklinde açıklanmıştır.’’[51] Kurumsal yönetim süreci, kapsamlı birçok süreçten oluşan bir yapı ya da bileşimdir. Bu yapı ve bileşimlere; etik ile ilgili

[48] G. Yurtsever, 2015, s. 99.

[49] **Worldcom Skandalı**: ABD’nin ikinci büyük şehirlerarası telekomünikasyon şirketi WorldCom’un 2001 yılında yaptığı 1.4 milyar dolarlık ve 2002 yılının ilk 3 ayında yaptığı 130 milyon dolarlık kârın doğru olmadığı ortaya çıktı. http://arsiv.ntv.com.tr/news/160390.asp, **Enron Skandalı**: Enron Skandalı olarak anılan ve Enron Şirketi’nin iflas etmesi ile sonuçlanan olaylar zinciri temel olarak, şirketin olduğundan daha kârlı gösterilmesi için muhasebe kayıtlarında yapılan hileler ve bu hilelerin denetim şirketi Arthur Andersen tarafından gizlenmesi olarak özetlenebilir. https://businessalignment.weebly.com/home/2921559

[50] Kayahan Tüm, Kurumsal Yönetim, İç Denetim ve İç Denetimin Kalitesi: Kalite Güvence ve Geliştirme Programı, **Çukurova Üniversitesi İİBF Dergisi**, Aralık 2013, C.17, S.2, s. 93-112, http://dergipark.ulakbim.gov.tr/cuiibfd/article/view/5000136769/5000125669

[51] IIA, **Özel Sektörde Kurumsal Yönetişimin Değerlendirilmesi**, UMUÇ, Uygulama Rehberi, Temmuz 2012, TİDE (Çev.), s. 5, https://www.tide.org.tr/

amaç ve programlar, bilgi teknolojileri yönetimi, misyon ve değerler, işe alım eğitim süreçleri, davranış kuralları, performans yönetimi, risk ve kontrol iletişimi örnek verilebilir. Ayrıca İK ve RY süreçleri de KY süreçlerinin bir parçasıdır.

2.2. Kurumsal Yönetimin Temel İlkeleri

KY uygulamaları kurumların bulundukları sektörel ve kültürel koşullardan etkilenir. Her ülkenin içinde bulunduğu farklı faktörler vardır. (hukuk sistemi, kurum kültürü vd.) Bu yüzden standart bir kurumsal yönetim metodolojisinden söz etmek pek mümkün değildir. Ancak tüm KY anlayışlarının temelinde yatan dört prensip vardır. Eşitlik, şeffaflık, hesap verebilirlik ve sorumluluk kavramları ortak ilkeler olarak KY uygulamalarının temelini teşkil etmektedir. Bu temel ilkeler hem hissedarların haklarını korurken aynı zamanda toplumsal normlara da uyumu sağlamaya yardımcı olur.[52]

Adillik: Kurum yönetiminin bütün hissedarlara eşit davranmasının tanımıdır. Azınlık hisseye sahip kişiler ile büyük yatırım sahibi kişilerin eşit haklara sahip olması gerekir.

Şeffaflık: Kurum yönetiminin kamuoyunun bilmesi gereken bilgileri şeffaflık çerçevesinde doğru biçimde paylaşması gerekir.

Hesap Verebilirlik: Yönetim kurulu, üst yönetim organlarının performansını izleme görevine sahiptir. Bu konuda kurum içinden bağımsız güvence sağlayıcılara güvenir ve hesap verilebilirliğin sağlanmasını destekler.

Sorumluluk İlkesi: Kurumun toplumsal normlara ve değerlere uyumlu faaliyet göstermek gerekir.

[52] Türkiye Kurumsal Yönetim Derneği, http://www.tkyd.org/tr/sss-kurumsal-yonetim-ilkeleri-nedir.html

2.3. Kontrol, İç Kontrol ve İç Kontrol Sisteminin Tanımı

Kontrol kavramının uluslararası iç denetim standartları ve uluslararası denetim terminolojisindeki anlamı ile ülkemizde algılanan tanımı arasında bazı farklılıklar bulunmaktadır. Ülkemizde kontrol kavramında genellikle kontrol etme eylemi anlaşılmaktadır. Bu eylem genelde işi yapan kontrol edenlerin birbirinden ayrı olması ilkesi ile birleşince kontrol kavramı gerçekleştirilerek sonlandırılan bir işlemin ilerleyen dönemlerde işlemi gerçekleştirenlerden başka ve bu görevle sorumlu bir kişi tarafından (kontrolör, denetçi vd.) yerine getirilen bir fonksiyon olarak algılanmakta kontrol kavramı bir işin gerçekleştirilmesi sürecine dahil edilmemekte, daha ziyade iş tamamlandıktan sonra devreye giren bir faaliyet olarak algılanmaktadır. Bu şekilde anlaşıldığında kontrol eylemi bir süreç değil, belli bir anda gerçekleştirilen ve sonuçlanan bir işlem olarak görülmektedir. UİDMUS'da kontrol kavramı sonradan gerçekleştirilen birey eylem olmayıp, bir işin planlanmasından organize edilmesine, gerçekleştirilmesine ve sonuçlandırılmasına kadar varan tüm işlem akışı içine giydirilmiş bir sürecin kontrol altında tutulmasını sağlayan sistematik bir süreci ifade etmektedir.[53]

(Kontrol ve kontrol süreci)[54], IIA terimler sözlüğünde şöyle açıklanmıştır. Kontrol: "Üst yönetim, yönetim kurulu ve ilgili diğer taraflarca riski yönetmek ve belirlenmiş amaç ve hedeflere ulaşma ihtimalini artırmak için yapılan her türlü eylem'' anlamına gelir. İdare amaç ve hedeflere ulaşılacağı konusunda makul güvence sağlanabilmesi için yeterli olacak faaliyetlerin yürütülmesini planlar, örgütler ve yönetir. Kontrol süreçleri ise "Risklerin, kurumun kabul etmeye gönüllü olduğu sınırlar içinde kalmasını sağlamak amacıyla tasarlanan ve işletilen kontrol çerçevesinin parçası olan faaliyet politika ve prosedürlerdir.''[55]

[53] Ç. Özbek, 2012, s. 136-137.
[54] ''Kontrol ve İç Kontrol'', ''Kontrol Süreçleri ve İç Kontrol Süreçleri'', ''İç Kontrol Sistemi, İç Kontrol Yapısı ve COSO İK Modeli'' kavramları kaynaklarda birbirlerinin yerine sıklıkla kullanılmaktadır.
[55] IIA, **Standartlar**, UMUÇ, 2017, s. 27.

İç kontroller, İKS'den belirgin olarak farklıdır. İç kontroller İKS'nin ağaçları iken, İKS ormandır. İç kontrol sistemi, iç kontrolleri yerleştirerek kurum içinde İK sağlar. İç kontroller, kontrol hedeflerine yönelik riskleri azaltacak şekilde organizasyondaki faaliyeti olumlu bir şekilde etkileyen mekanizmalar, kurallar, güvenlik önlemleri ve süreçlerdir. İç kontroller, kuruluşun faaliyetinin çeşitli yönlerini kontrol etmeye yardımcı olmak ve bu faaliyetin kontrol hedeflerine uygun olduğunu makul bir güvence altına almak için tasarlanmıştır. İK örnekleri aşağıdaki gibi örneklendirilebilir:[56]

• Yeni çalışanların referanslarının kontrol edilmesi,

• Finansal sistemler üzerinde çalışma saatlerinin sınırlandırılması,

• Her 6 ayda bir şifre değişikliklerinin yapılması,

• Her gün yedekleme yapılması.

COSO tarafından 1992 yılında geliştirilen ve 2013 yılında da yenilenen ‘‘COSO İç Kontrol Bütünleşik Çerçevesi’’ dünya genelinde kabul görmüş en iyi uygulamalardan biridir. Bu model dışında Kanada'da ‘‘Criteria of Control Board (CoCo)’’ ve İngiltere'de ‘‘Turnbull Raporu’’ gibi çeşitli raporlar ile bilgi teknolojileri alanında ‘‘Control Objectives for Information Technology (COBIT)’’ modeli tarzında yaklaşımlar vardır.[57]

[56] Internal Control System, http://www.objectivecontrols.com/internal_control_system.html
[57] D. Pehlivanlı, 2014, s. 31.

(COSO İK modeli)[58] iç kontrolü şöyle tanımlanmaktadır: "İç kontrol, işletmenin yönetim kurulundan ve tüm çalışanlarından etkilenen, aşağıda belirtilen amaçlara ulaşmak amacıyla makul bir güvence sağlamak için tasarlanmış bir süreçtir.''[59]

• Mali raporlamaların güvenilirliği,

• Faaliyetlerin etkililiği ve etkinliği,

• Yasalara ve kurum içi mevzuatlara uyum.

Kontrol Süreçleri: Riskin, bir kurumun kabul etmek isteyeceği seviyede kalması gayesiyle oluşturulan ve işletilen kontrol çerçevesinin bir parçası olan faaliyet, politika ve prosedürlerdir.[60]

COSO iç kontrol süreci ise; (kontrol ortamı - risk değerlendirme - kontrol faaliyetleri - bilgi ve iletişim - izleme) bileşenlerinden oluşur.

2.4. İç Kontrol ve İç Kontrol Sisteminin Amacı ve Önemi

İç kontroller, bir kurumda riskleri azaltma amacıyla faaliyet gösteren uygulama, prosedür, politika, süreç, sistem ve eylemlerdir. İKS ise, işletme genelinde amaç ve hedeflerin gerçekleştirilmesi amacı ile tasarlanan, tüm iç kontrolleri de kapsayan, aynı zamanda organizasyon, risk değerlendirmesi, iletişim ve iç denetimi de kapsayan bir yönetim aracıdır.[61]

---

[58] **COSO Modeli (COSO Model)**: COSO tarafından hazırlanan ve bir kurumun günlük faaliyetleri sırasında kurum içerisindeki mevcut ve olması gereken asgari İK uygulamalarının sistematik bir şekilde değerlendirilmesine olanak sağlayan bir İK modelidir. COSO Modeli İKS'ye ilişkin standartların temelini oluşturmaktadır. COSO;www.bumko.gov.tr/iç control; İDKK, **Kamu İç Denetim Terimler Sözlüğü**, http://www.idkk.gov.tr (Dünya genelinde birçok İK modeli bulunmakta ve uygulanmaktadır. Bu çalışmada ülkemizde ve uluslararası alanda en çok tercih edilen kontrol modellerinden olan COSO İK modeli incelenmiştir. Ayrıca bu çalışmada ''Model'' ve ''Çerçeve'' kavramları birbirlerinin yerine kullanılmıştır)

[59] COSO, **Internal Control Integrated Framework**, 1992, s. 133'den aktaran Ç. Özbek, 2012, s. 402.

[60] IIA, **Standartlar**, UMUÇ, 2017, s. 27.

[61] Bertan Kaya, **İç Kontrolün Özü Nedir**, 2014, http://bertankaya.net/?p=1104

İK tek veya anlık bir eylem veya koşul olmayıp sürekli devam eden tüm süreçlerin içerisine yerleştirilmiş uygulamalardır. İç kontrolde en önemli unsur insandır. İK; yönetim kurulu, yöneticiler ve diğer personeller tarafından etkilenir ve bir kurumda insanların söyledikleri ve yaptıklarıyla gerçekleştirilir. İK'den sağlanacak fayda mutlak değil makuldür. Ne kadar iyi dizayn edilsin veya işletilirse işletilsin kurum hedeflerinin gerçekleştirilmesi konusunda yönetim kurulu ve üst yönetime sadece makul bir güvence sağlar. Özellikle bir veya daha fazla kişinin kasıtlı eylemleri ile bazı kontrol faaliyetlerinin geçersiz kılınması her zaman olasıdır. Üst düzey yöneticiler ise her zaman iç kontrolün etkilerini sınırlandırabilme veya onu aşabilme gücüne sahiptir. İç kontrol kurum hedeflerinin gerçekleştirilmesine odaklanır.[62]

2.5. COSO Komitesi ve COSO İç Kontrol Modeli

Son yıllarda yaşanan hileli raporlamalar, İK kavramının yeniden düzenlenmesi gereğini ortaya çıkarmış bu amaçla COSO komitesi kurulmuştur. COSO; İK, KRY ve suiistimali önleme alanlarında geniş rehberler hazırlamak suretiyle ve fikir önderliği yapmak amacıyla, ABD'de bazı özel sektör kuruluşlarının sponsorluğunda 1985 yılında kurulmuştur.[63]

COSO komitesi 1992 yılında İç Kontrol Bütünleştirilmiş Çerçeve (Internal Control Integrated Framework) isimli bir rapor geliştirmiştir. Bu rapor ile iç kontrolün temel prensiplerini ortaya koyan bir model oluşturulmuştur. COSO komitesi tarafından 1992 yılında oluşturulan bu iç kontrol çerçevesi zaman içerisinde değişen koşulları da dikkate

[62] COSO, **Internal Control Integrated Framework**, 1992, s. (14-15)'den aktaran Ç. Özbek, 2012, s. 403-404.
[63] COSO; **COSO 2013 İç Kontrol Çerçevesi**, https://denetimsitesi.wordpress.com/2014/08/15/coso-2013-ic-kontrol-cercevesi-3/

alınarak, ihtiyaçlara cevap vermekte zorlanınca, 2013 yılında mevcut model COSO tarafından revize edilerek yeniden yayınlanmıştır.[64]

COSO'nun ortaya koyduğu İK modeli yeni baştan ortaya konulan bir model değildir. COSO'nun alt bileşenlerini oluşturan kontrol ortamı kontrol faaliyetleri gibi hususlar o ana kadar muhtelif meslek kuruluşları tarafından tanımlanmıştır. COSO'nun en önemli katkısı, üzerinde tartışılan ancak net bir tanımı olmayan İK kavramının geniş bir katılımla net bir tanımını yapabilmiş olması, etkin bir İKS'yi hangi unsurların oluşturduğunu ortaya koyabilmiş olması ve son olarak da kontrol sistemlerinin etkinliğini değerlendirmek isteyen firmalara bunu yapabilmelerini sağlayacak bir araç veya kriterler seti sunmuş olmasıdır. Nitekim COSO modeli etkilerini gerek özel kesimde gerek kamu kesiminde göstermiştir. Örn: Uluslararası Sayıştaylar Birliği (INTOSAI) kamu kesimine yönelik geliştirdiği İK standartlarında COSO bileşenlerini esas almıştır. Uluslararası Ödemeler Bankası (BIS) tarafından bankacılık kesiminde etkin bir İKS'nin unsurlarının tanımlanmasında COSO modelinin bileşenleri detaylı aynı mantık silsilesi içerisinde kullanılmıştır.[65]

Grafikle Gösterim: COSO çerçevesi, Şekil 3'deki gibi satır kesit ve sütunlardan oluşan bir küp olarak gösterilebilir.[66] Satırlar beş bileşendir, kesitler üç faaliyet kategorisidir ve sütunlar kurumun birimleri yada faaliyetleridir. Sütunlar aynı zamanda kurumu bir bütün olarak gösteren tek bir boyut olarak da görülebilir. Hedeflerin kurumun belirlemiş her faaliyetine ve işletme birimine uygun olup olmadığı incelenmelidir. Her faaliyet/birim ve hedef kombinasyonunun beş bileşenin her birini ele alması gerekir.[67]

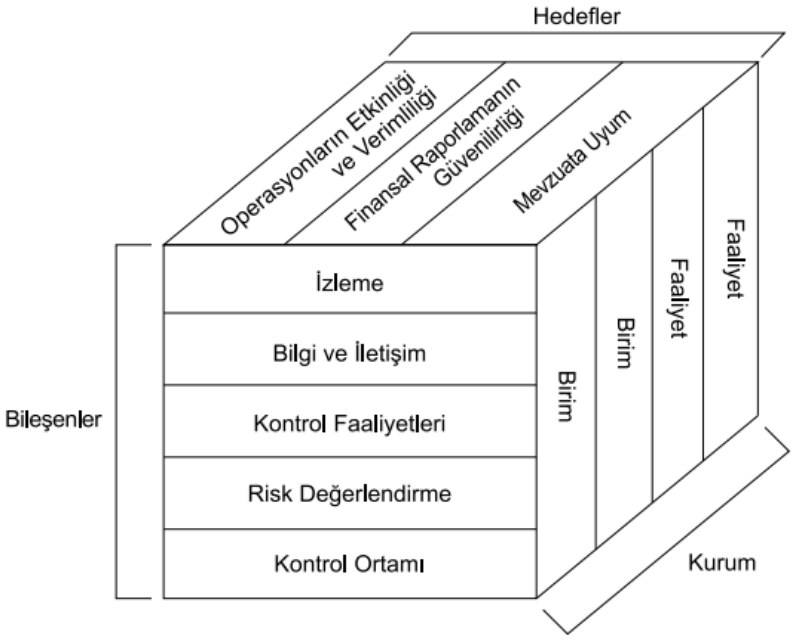
---

[64] COSO; **COSO 2013 İç Kontrol Çerçevesi**, https://denetimsitesi.wordpress.com/2014/08/15/coso-2013-ic-kontrol-cercevesi-3/

[65] COSO, **Internal Control Integrated Framework Exposure Draft**, Aralık 2011, https://www.coso.org/' dan aktaran Ç. Özbek, 2012, s. 395.

[66] COSO; Gleim Publications, **Control Framework and Fraud,** Study Unit Four, 2015, TİDE (Çev.), s. 4, https://www.gleim.com/

[67] a.g.e.



Şekil 3: COSO İç Kontrol Çerçevesi

2.5.1. COSO İç Kontrol Modeli Bileşenleri

COSO İç kontrol Modeli aşağıda açıklanan beş bileşenden oluşmaktadır. Bileşenler hep birlikte iç kontrol amaçlarının gerçekleştirilmesine yönelik belirlenmiştir. Bu beş bileşenden kontrol ortamı bileşeni diğer tüm bileşenler için temel oluşturur ve özel bir konuma sahiptir.

2.5.1.1. Kontrol Ortamı

Kontrol ortamı, kuruluş genelinde iç kontrole ilişkin temel oluşturan standartlar, süreçler ve yapılardan oluşur. Yönetim kurulu ve üst düzey yönetim, beklenen davranış standartlarını da içeren iç kontrolün önemi ile ilgili en üst noktayı oluşturmaktadır. Yönetim, organizasyonun çeşitli kademelerindeki beklentileri güçlendirir. Kontrol ortamı organizasyonun bütünlük ve etik değerlerini içerir. Yönetim kurulunun; yönetişim denetim sorumluluklarını yerine getirmesini sağlayan parametreler, yetki ve sorumluluklar organizasyon yapısı ve görevlendirilmeler, yetkin kişilerin kuruma kazandırılması, geliştir-

mesi ve kurumda tutulma süreci, performansa ilişkin hesap verebilirliği artırmak için performans önlemleri, teşvik ve ödül konularında hassas davranma gibi konulardan oluşan kontrol ortamı, İKS üzerinde yaygın bir etkiye sahiptir.[68]

Kontrol ortamı kurum çalışanlarının kontrol farkındalıkları üzerinde önemli bir etkiye sahiptir. Kontrol ortamını; dürüstlük, etik değerler, çalışanlarının yetkinliği ve yeterliliği, yönetimin iş yapma felsefesi ve çalışma usulü, organizasyonun yetki ve sorumluluk dağılımı oluşturur.[69]

2.5.1.2. Risk Değerlendirme

COSO çerçevesinde risk değerlendirme bileşene ait 7. prensibin odak noktaları şu şekilde açıklanmıştır. ‘‘Risk değerlendirme bileşeninde kurum, hedeflerine ulaşmada engel oluşturacak riskleri tanımlar. Bu riskleri nasıl yönetileceğini belirlemek için temel olarak riskleri analiz eder.’’ Bu anlamda odaklandığı noktalar aşağıdaki gibidir:[70]

• Kurum, yan kuruluş, bölüm, işletim birimi ve işlevsel yönetim seviyelerinde riskler tanımlanır ve değerlendirilir.

• İç ve dış faktörler analiz edilir. Tanımlanan risklerin, hem iç hem de dış etkenleri ve bunların hedeflere ulaşma üzerindeki etkilerini göz önünde bulundurulur.

• Belirlenen risklerin önem derecesi tahmin edilir ve analiz edilir.

• Risklere nasıl cevap verileceği belirlenir. Risk değerlendirmesi, riskin nasıl yönetilmesi gerektiği (kabul etme, önleme, azaltma veya paylaşma) seçeneklerini dikkate alır.

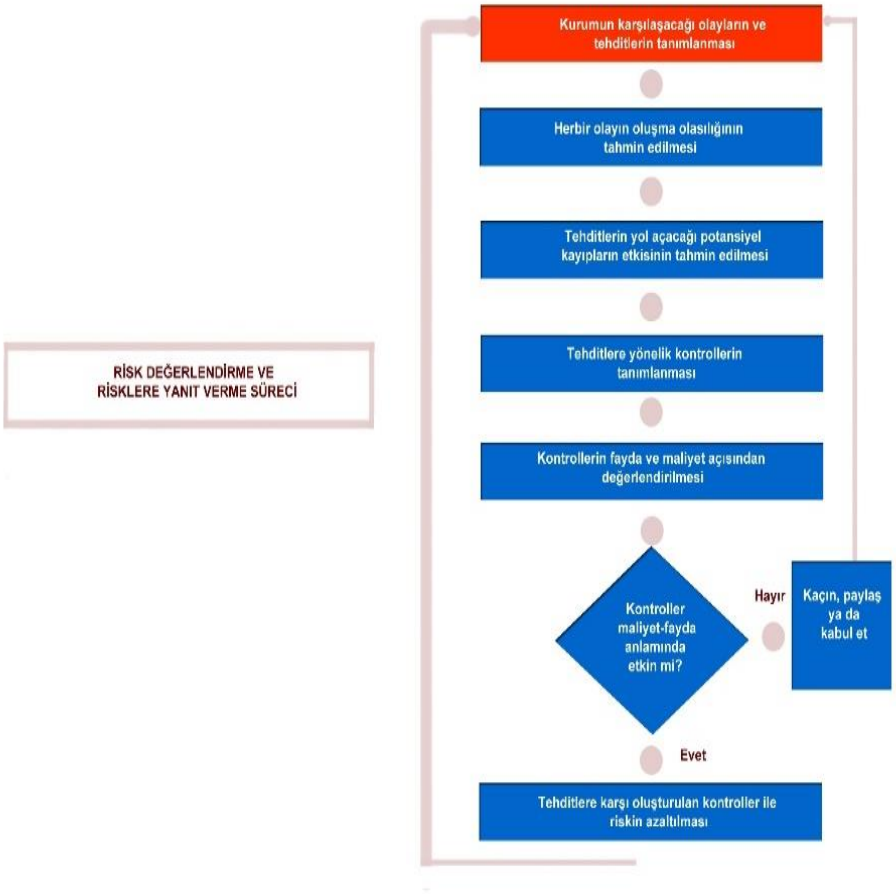
---

[68] Oduware Uwadiae, Deloitte, COSO An Approach to Internal Control Framework, **Financal Reporting Deloitte**, https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/audit/Financial%20Reporting/ng-coso-an-approach-to-internal-control-framework.pdf

[69] COSO, **Internal Control - Integrated Framework**, 1992, s. 5’den aktaran Ç. Özbek, 2012, s. 408.

[70] KPMG, **Risk Assesment**, COSO Framework, 2015, https://www.isaca.org/chapters1/phoenix/events/Documents/KPMG-COSO-Presentation.pdf, s. 21.

Risk değerlendirme bileşeni çalışmanın son bölümünde ayrıntılı olarak açıklanmıştır.[71]



Şekil 4: Risk Değerlendirme ve Risklere Yanıt Verme Süreci

Kaynak:https://www.coursehero.com/file/p2mr1kv/ACC-444-Enterprise-Process-Analysis-27-RISK-ASSESSMENT-AND-RISK-RESPONSE-COSO/

2.5.1.3. Kontrol Faaliyetleri

Kontrol faaliyetleri, hedeflere ulaşılmasında risklerin azaltılmasına yönelik yönetim direktiflerinin gerçekleştirilmesini sağlayan politikalar ve prosedürler yoluyla belirlenen eylemlerdir. Kontrol faaliyetleri kurumun her düzeyinde, iş süreçleri içindeki çeşitli aşamalarda ve teknoloji ortamında gerçekleştirilir.[72] Teknoloji kullanmadan gerçekleştirilen kontrollerde vardır. (Örn: Manuel Kontroller vd.)

[71] Geniş bilgi için bkz. Bölüm: (5.1.).
[72] Oduware Uwadiae, a.g.m.

Kontrol faaliyetlerine örnek olarak (yetkilendirmeler, onaylamalar, görevler ayrığı, önleyici kontroller, yönlendirici kontroller) verilebilir.

2.5.1.4. Bilgi ve İletişim

İşletmenin hedeflerine ulaşılmasının desteklemesi, İK sorumluluklarını yerine getirmesi için bilgi gerekmektedir. İletişim; gerekli bilgileri sağlamak, paylaşmak ve elde etmek için sürekli, tekrarlayan bir süreçtir. İç iletişim; bilginin kuruluş genelinde yayılması, kurumdan yukarıya doğru, aşağıya doğru ve kurum boyunca yayılması için kullanılan araçtır. Personelin üst yönetimden, kontrol sorumluluklarının ciddiye alınması gerektiğinin açık bir mesajını almasını sağlar. Dış iletişim iki yönlüdür. İlgili dış bilginin gelen iletişimini sağlar ve gereksinimlere ve beklentilere yanıt olarak dış taraflara bilgi sağlar. İç kontrol çerçevesinin bilgi ve iletişim bileşeni, iç kontrolün tüm bileşenlerinin işleyişini desteklemektedir. Diğer bileşenlerle birlikte bilgi ve iletişim, kurum içi ve dışı raporlamayla ilgili hedefler de dahil olmak üzere kuruluşun hedeflerine ulaşılmasını destekler. Bilgi ve iletişim kontrolleri, kurumun İKS içinde doğru bilgiyi kullanma ve İK sorumluluklarını yerine getirme kabiliyetini desteklemektedir.[73]

2.5.1.5. İzleme

İzleme faaliyetleri; sürekli değerlendirmeler, ayrı değerlendirmeler veya her ikisinin bir kombinasyonu şeklinde yapılabilir. İç kontrolün beş bileşenden her birinin, her bileşen içindeki ilkeleri etkileyen kontroller de dahil olmak üzere mevcut olup olmadığını ve faal olup olmadığını tespit etmek için kullanılır. İşletmenin farklı seviyelerinde iş süreçlerine yerleştirilen sürekli değerlendirmeler, zamanında bilgi sağlar.

[73] http://controlsframework.com/info_communication.php

Periyodik olarak yapılan ayrı değerlendirmeler, risklerin değerlendirilmesine, devam eden değerlendirmelerin etkinliğine ve diğer yönetim hususlarına bağlı olarak kapsam ve sıklığa göre değişiklik gösterir. Bulgular; düzenleyiciler, standart belirleme organları veya yönetim ve yönetim kurulu tarafından belirlenen kriterlere göre değerlendirilir ve eksiklikler yönetim ve yönetim kuruluna uygun şekilde bildirilir. İzleme faaliyetleri, iç kontrolün beş bileşeninin her birinin mevcut ve işlevsel olup olmadığını değerlendirir. İzleme, kurumun iç kontrolün etkinliğini değerlendiren kilit girdidir. Gerektiğinde, İKS'nin etkililiği konusundaki iddialara değerli destek sağlar.[74]

[74] http://controlsframework.com/monitoring.php

ÜÇÜNCÜ BÖLÜM

RİSK VE RİSK YÖNETİMİ

3.1. Risk Tanımı

Risk kavramına ilişkin farklı tanımlar mevcuttur. IIA riski şöyle açıklamıştır. Risk: "Amaçlara ulaşılması üzerinde etkisi olacak bir olayın meydana gelme ihtimalidir."[75]

Risklerin yaratacağı sonuçların bir miktar fırsatları da içinde barındıracağı unutulmamalıdır. Risk, planlanan amaçlardan sapmayı ortaya çıkaran her türlü durumdur. Tehlike ve belirsizliği kapsamaktadır bunun yanında fırsatları da barındıran bir kavramdır. Beklenmeyen olaylar tehlikeyi, değişimler belirsizliği, çeşitli tehlikeleri avantaja çevirebilme yeteneği de fırsatları beraberinde getirmektedir.[76]

3.2. Risk Çeşitleri

Bir kurumun maruz kalabileceği riskler çok farklı şekillerde gruplandırılabilir. Kurumun yapısal ve sektörel özellikleri bu gruplandırmayı önemli miktarda etkileyecektir. Riskleri gruplandırmanın birçok yolu olmasına rağmen en yaygın metot riskleri dört ana grup altında toplamaktır. Bunlar; finansal riskler, operasyonel riskler, stratejik riskler ve dış çevre riskleridir. Aşağıda dört başlıkta risk çeşitleri açıklanmıştır:[77]

---

[75] IIA, **Standartlar**, UMUÇ, 2017, s. 28.

[76] Sezer Bozkuş Kahyaoğlu, **Kurumsal Risk Yönetimi Standartları**, Grant Thornton, http://www.gtturkey.com/ud_objs/pdf/etknlk/musiad_risk_yonetimi_sunumu.pdf, s. 6.

[77] Türk Sanayicileri ve İş Adamları Derneği (TÜSİAD), Kurumsal Risk Yönetimi, **TÜSİAD Yayını**, Yayın No: T/2008-02/452, 2008, http://tusiad.org/tr/yayinlar/raporlar/item/download/3470_3def5dc2dc47e5faf697ba2bcb541181 s. 19-20.

Finansal Riskler: Finansal durumların oluşturduğu riskleri tanımlar.

Operasyonel Riskler: Bir işletmenin temel işlevsel fonksiyonlarını yerine getirirken karşılaşabileceği riskleri tanımlar. Satış, ürün geliştirme, marka yönetimi gibi konularda meydana gelebilecek riskler örnek olarak verilebilir.

Stratejik Riskler: Bir işletmenin stratejik hedeflerine ulaşmasına engel olacak muhtelif risklerin tanımıdır.

Dış Çevre Riskleri: Bu sınıfta yer alan riskler kurum faaliyetlerinden bağımsız ancak kurumu etkileme olasılığına sahip risklerdir. Sektör uygulamalarındaki değişiklikler, yasa ve politika değişiklileri gibi konular örnek verilebilir.

3.3. Risk Yönetiminin Tanımı ve Amacı

RY, IIA'nın yaptığı tanımında: ''İşletmenin amaçlarını gerçekleştirmek üzere makul bir güvence elde etmek amacıyla, mevcut olay ve durumları belirleme, değerlendirme, yönetme ve kontrol etme süreci şeklinde açıklanmıştır.''[78]

RY aşağıdaki temel faaliyetleri içerir:[79]

- RY'nin nasıl icra edileceğinin planlanması ve risklerin belirlenmesi
- Risklerin etki ve olasılıklarının tahmin edilmesi
- Risklerin önem derecesinin belirlenmesi
- Kritik öneme sahip risklerin belirlenmesi
- Risklerin temel nedenlerinin belirlenmesi
- Riskleri azaltmaya yönelik faaliyetlerin planlanması ve uygulanması
- İzleme ve iyileştirme faaliyetleri

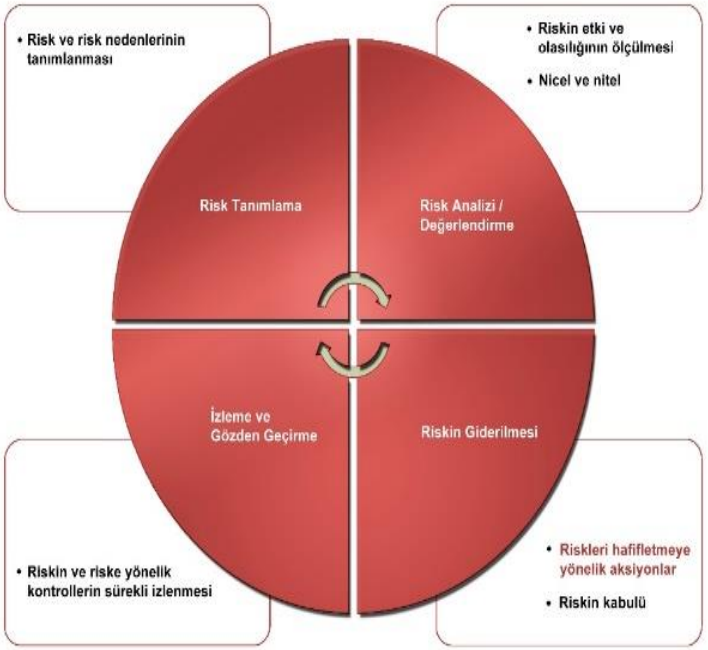
[78] IIA, **Standartlar**, UMUÇ, 2017, s. 28.

[79] Meryem Fıkırkoca, **Bütünsel Risk Yönetimi**, KalDer Yayınları, Ankara, 2003, s. (14-15)'den aktaran Demet Kalyoncu, **Risksiz Risk Yönetiminin Alternatif Yolları**, Yüksek Lisans Tezi, Okan Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2013, s. 17.

Risk Yönetim Süreçleri: Risk yönetim süreçleri, kurumun hedeflerine ulaşması konusunda makul güvence sağlayabilmek amacıyla, riskleri tespit etmek, değerlendirmek ve risk aksiyonlarını uygulamak için oluşturduğu, uygulamaya koyduğu süreçler anlamına gelir.[80]

RY süreci; risklerin değerlendirilmesi (risklerin tanımlanması, analiz edilmesi, değerlemesi)[81], riske karşı yapılacak mücadele yönteminin belirlenmesi (riske cevap verilmesi)[82] varsa risklerin doğuracağı fırsatların tespit edilmesi ve uygulanan yöntemlerinin kontrolü ve gözetimini içeren bir süreçtir. Bu süreç, kimi kurumlarda yazılı ve sistematik, kimi kurumlarda ise informel hatta kendiliğinden gelişen ve farkında olmadan günlük olayların bir parçası olabilir. Her kurumda risklerin belirlenme şekli ve risklerin nasıl bertaraf edildiği, kurumların farklı yapıları nedeniyle değişiklik gösterir.

[80] IIA, **İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol**, UMUÇ, Pozisyon Raporu, TİDE (Çev.), 2009. s. 8.
[81] Geniş bilgi için bkz. Bölüm: (2.5.1.2.), (4.4.1.4.), (5.1.).
[82] Geniş bilgi için bkz. Bölüm: (2.5.1.2.), (4.4.1.5.).



Şekil 5: Risk Yönetim Süreci

Kaynak: http://www.moresecure.ca/risk-management/

3.4. Risk Yönetiminin Kapsamı

Herhangi bir riskle karşı karşıya kalma ihtimali olmayan bir sektör veya iş kolunun olması mümkün değildir. Bütün kurumlar faaliyetlerine ve kurumun geleceğine yönelik olumsuz sonuçlar doğurabilecek risklerin neler olduğunu ve bunlara karşı ne tür önlemler almaları gerektiğini bilmek zorundadır. Risk yönetimi faaliyetlerinin kapsamı kurumdan kuruma değişiklik gösterecektir. RY firmanın sadece en önemli birkaç riskini kapsayacak şekilde az sayıda kişi tarafından ve genelde üst düzey yöneticilerin liderliğinde gerçekleştirilebileceği gibi tüm çalışanların katılımıyla formel bir yapıya sahip KRY uygulamaları şeklinde de sürdürülebilir. Bu durumda firma sadece önemli gördüğü risklere üst yönetim seviyesinde odaklanacak göreceli olarak önemsiz gördüğü

risklere açık olmayı tercih etmiş olacaktır. KRY, RY uygulamalarının firmanın sadece en önemli değil olası tüm risklerini sistematik bir şekilde ele aldığı yönetim kurulu ve üst düzey yöneticilerin gözetim sorumluluğu altında spesifik risk birimleriyle desteklenen ve tüm çalışanların katılımıyla gerçekleştirilen en geniş kapsamlı halini yansıtmaktadır.[83]

RY farklı kurumlarda farklı şekillerde uygulanabilir. RY büyük bir holdingde farklı, orta ölçekli bir şirkette daha farklı şekilde yöntem ve yaklaşımlar ile uygulanan bir yönetim aracıdır. Ancak hangi şekilde yapılırsa yapılsın RY'nin temel prensipleri değişmez. RY amaç ve hedeflerle doğrudan bağlantılıdır. Bir işletmenin amaç ve hedefleri yoksa o işletmede bir RY'den bahsedemeyiz. Risk ve risk yönetimi için somut amaç ve hedeflerin var olduğu bir yapı olması gerekir.[84]

3.5. Risk Yönetim Modelleri

Geçmişten günümüze RY modelleri zaman içerisinde önemli ölçüde gelişim göstermiştir. RY; riskleri olumsuz algılayan, fiziksel kayıplara odaklanılan, sigortalama yöntemini tercih eden geleneksel risk yönetiminden; risklerin kuruma olan maliyetlerinin azaltılması, kurumun istediği risk/kazanç dengesine ulaşmasına yardımcı olan gelişmiş risk yönetimine (finansal risk yönetimi) doğru gelişim göstermiş ve son olarak stratejik risk yönetimi modeli yaklaşımıyla kuruma özel risk evreninin hazırlandığı ve sistematik bir yapıda risklerin tüm kurum çapında yönetildiği kurumsal risk yönetim anlayışına dönüşmüştür. Böylece KRY dünya genelinde kabul gören bir yöntem haline gelmiştir.

[83] Ç. Özbek, 2012, s. 242-243.
[84] Bertan Kaya, **Risk Yönetim Planı Nasıl Oluşturulur**, 2015, http://bertankaya.net/?p=1104

Tablo 1: Risk Yönetim Modelleri

Geleneksel Risk Yönetimi (Traditional)	**Gelişmiş Risk Yönetimi (Progressive/Advanced)**	**Stratejik Risk Yönetimi (Strategic)**
Riskin Tanımlanması ve Riskin Yönetimi	Finans Riskleri	Kurumsal Risk Yönetimi
Kayıpların Önlenmesi	İş Sürekliliği	Riskin İndekslenmesi
Analizler, Sigortalama ve Riskin Transfer edilmesi	Riskin Toplam Maliyeti Eğitim ve İletişim	Teknolojinin Kullanılması

Kaynak: Kate Lark, Paul L. Walker, **Risk Management, Enterprise Risk Management**, 2008.

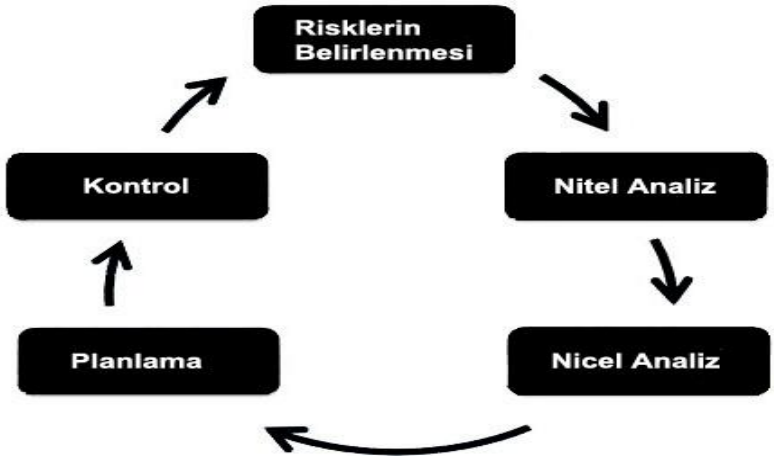
Risk yönetiminde, riskleri kötü algılayan ve yönetmekten ziyade sigortalama yöntemini tercih eden geleneksel risk yönetim sisteminden, risklerin kuruma olan maliyetlerinin azaltılmasına odaklanan gelişmiş RY sistemine geçilmiştir. Günümüzde işletmeler risklerin yaratacağı olayların fırsatları da barındırabileceğini savunan KRY sistemine yönelmiştir.[85]

3.5.1. Geleneksel Risk Yönetimi

Her kurumda riskler operasyonlarla devam ederken anlık ya da periyodik bir zaman diliminde değerlendirilip yönetilebilir. Geleneksel risk yönetimi modeli, fiziksel kayıplara neden olacak risklerin belirlenmesi, analiz edilmesi ve çeşitli kontrol

[85] Ruveyda Kızılboğa, Geleneksel Risk Yönetiminden Kurumsal Risk Yönetim Sistemine Geçiş, **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 2012, S.16(3): 297-316, s. 306.

faaliyetleriyle azaltılmasına yönelik uygulanan risk yönetim modelidir. Geleneksel risk yönetiminde riskler kurum genelinde bir bütün olarak ele alınmadan birim ya da operasyonel süreç bazlı değerlendirilerek, ayrı ayrı silo şeklinde yönetilmektedir. Günümüzde çoğu küçük ölçekli veya büyüme aşamasında olan işletmeler, daha çok operasyonel düzeyde işlem yaptıkları ve henüz stratejik bir risk yönetimi oluşumu tamamlayamadıkları için strateji odaklı bir risk yönetimi uygulayamamaktadır.



Şekil 6: Geleneksel Risk Yönetimi Süreci

Kaynak: Ken Rubin, **Agile & Risk Management: The Role of Traditional Risk Management**, 2014, http://www.innolution.com/blog/agile-risk-management-the-role-of-traditional-risk-management

3.5.2. Gelişmiş (Finansal) Risk Yönetimi

İleri düzey risk yönetim modeline, finansal risk yönetim modeli de denilebilmektedir. Risklerin azaltılmasında sigortalama yönteminin yerine, daha çok finansal tekniklerin kullanıldığı, geleneksel risk yönetimine kıyasla daha proaktif bir yaklaşımla, yönetim taleplerini de dikkate alarak bütünleşik bir yapıda risklerin yönetilmesidir. Risk olumsuzluktan ziyade, gider olarak görülür ve riskin oluşturacağı olumsuzlukların maliyetlerinin azaltılmasına odaklanılır. Finansal risk yönetimi ayrı bir değerlendirme gerektirse de, geleneksel risk yönetimin bir parçası olarak düşünülebilir.

3.5.3. Stratejik Risk Yönetimi

Kuruluşların risk yönetimini sistematik ve etkili bir şekilde uygulamasına yardımcı olmak için dünya genelinde bir takım standartlar geliştirilmiştir. Bu standartlar, çerçeveler, süreçler ve uygulamalar konusunda ortak bir görüş oluşturmak ister ve genellikle kabul görmüş uluslararası standart organları veya sanayi grupları tarafından belirlenir. Risk yönetimi hızlı bir disiplindir ve standartlar düzenli olarak tamamlanır ve güncellenir. Bir standarda uyulması, düzenleyiciler veya sözleşme tarafından istenebilir ancak standartlar normalde gönüllüdür. Yaygın olarak kullanılan standartlar şunlardır:[86]

- ISO 31000: 2009 - Risk Yönetim İlkeleri ve Kuralları
- Risk Yönetim Standardı - Institute of Risk Management (IRM) - İngiltere
- **COSO 2004 Kurumsal Risk Yönetimi - Entegre Çerçeve**[87]
- (OCEG) ‘‘Kırmızı Kitap’’ 2.0: 2009 - Yönetişim, Risk ve Uyumluluk Yetenek Modeli

[86] https://www.theirm.org/the-risk-profession/risk-management.aspx

[87] Bu çalışmada, IIA’nın yayınladığı dökümanlarla, COSO komitesinin yayınladığı COSO İK ve COSO ERM çerçeveleri incelenmiş; Enterprise Risk Management (ERM) ve Kurumsal Risk Yönetimi (KRY) kısaltmaları birbirlerinin yerine kullanılmıştır.

DÖRDÜNCÜ BÖLÜM

KURUMSAL RİSK YÖNETİMİ

4.1. Kurumsal Risk Yönetiminin Tanımı ve Amacı

KRY, RY anlayışının metotlarının spesifik görev ünitelerine ve günlük operasyonel faaliyetlere entegre edilmesidir. KRY günümüzde uygulanması gereken en iyi risk yönetim uygulaması olarak kabul edilmektedir. OECD raporlarında halen devam eden global krizlerin nedenleri arasında finans kuruluşlarının aşırı risk iştahının olduğu bu kuruluşların risk iştahları ile kurumsal stratejilerinin uyum içerisinde olmadığı, yönetim kurumu seviyesinde RY'nin önemi konusundaki farkındalığının yetersiz olduğu, risklerin kurum çapında yönetilmediği sıklıkla ifade edilmektedir. "Enterprise Risk Management", ''Corporate Risk Management'', ''Integrated Risk Management'' gibi terimler Türkçeye "Kurumsal Risk Yönetimi'' olarak çevrilmiştir.[88]

Geleneksel risk yönetim sisteminin dar kapsamından çıkılarak, işletmelerin her türlü faaliyet alanında karşı karşıya kalabilecekleri riskleri (stratejik, faaliyet, uygunluk, raporlama, teknolojik ve personel gibi) bir bütün olarak değerlendirmesi gereksinimi oluştu. Böylece dünya genelinde KRY anlayışı ortaya çıkmıştır.[89]

KRY için küresel anlamda en çok kabul görmüş tanım COSO tarafından yapılmıştır. COSO'ya göre KRY tanımı şöyledir: "KRY, şirketi etkileyebilecek potansiyel olayları tanımlamak, riskleri şirketin kurumsal risk alma profiline uygun olarak yönetmek ve şirketin hedeflerine ulaşması, finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ve uygulanabilir yasa ve düzenlemelere uygunluk

---

[88] PricewaterhouseCoopers Türkiye Danışmanlık Hizmetleri, **Her Yönüyle Kurumsal Risk Yönetimi**, 2006, http://docplayer.biz.tr/370845-Her-yonuyle-kurumsal-risk-yonetimi.html

[89] Ruveyda Kızılboğa, **Kurumsal Risk Yönetimi Odaklı İç Denetim ve İstanbul Büyükşehir Belediyesi İçin Bir Model Önerisi**, Marmara Belediyeler Birliği Yayını, İstanbul, 2013, S.76, s. 70.

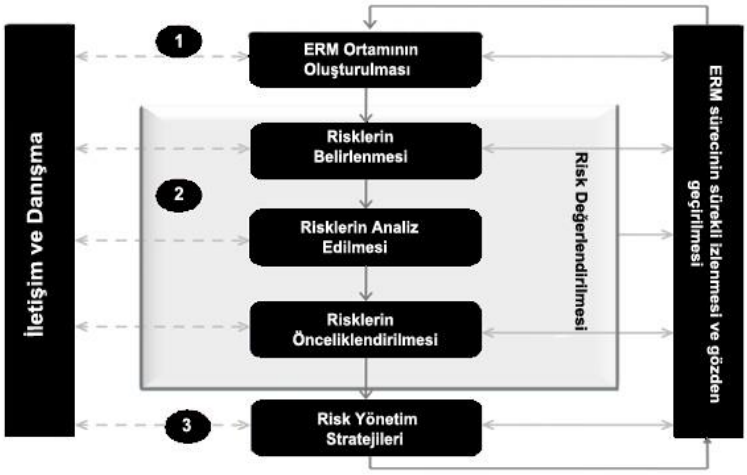
amaçlarına ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; şirketin yönetim kurulu, yöneticileri ve tüm diğer çalışanları tarafından etkilenen ve iç kontrolü de kapsayarak belirli bir strateji içinde tüm işletme çapında uygulanan sistematik bir süreçtir."[90]

İşletmelerin hedefleri dört gruba ayrılır. **Stratejik hedefler**: Kurumun misyonu ve vizyonu doğrultusunda üst seviye hedeflerini, **Faaliyet hedefleri**: Mevcut kaynakların etkili ve verimli kullanılmasıyla ilgili hedefleri, **Raporlama hedefleri**: Finansal raporlamaların güvenilirliği ile ilgili hedefleri, **Uyum hedefleri**: Yürürlükteki yasa ve yönetmeliklerle uyumun sağlanması ile ilgili hedefleri tanımlamaktadır. KRY hedeflere ulaşmada tıpkı iç kontrol gibi sadece makul bir güvence sağlar. KRY, kurumun her seviyesinde (işletme, bölüm, şube, iş birimleri seviyesinde) yürütülmektedir.[91]

Kurumsal Risk Yönetimi Süreci: KRY süreci; ERM ortamının oluşturulması, risklerin değerlendirilmesi, risk yönetim stratejilerinin belirlenmesi ve uygulanması, ERM sisteminin sürekli izlenmesi, gözden geçirilmesinden oluşan sistematik ve strateji odaklı bir süreçtir. Kurum içerisinde etkin bir RY'nin kurulabilmesi için öncelikle ERM ortamının oluşturulması dış (ticari ve sosyal çevre, finansal politik çevre vd.) ve iç unsurların (şirket kültürü, organizasyon yapısı vd.) belirlenerek bir ERM çerçevesi ve risk alma isteğinin belirlenmesi gerekir. İkinci aşama risklerin değerlendirilmesidir. Riskler belirlendikten sonra analiz edilerek (etki/olasılık)[92] yönünden ölçülür ve önceliklendirilir. Son aşama ise risklere karşı nasıl cevap verileceğinin belirlenmesi yani risklerin nasıl bir

[90] COSO, **Enterprise Risk Management Integrated Framework**, 2004'den aktaran Ş. Güneş, 2009, s. 13-14.
[91] COSO, **Enterprise Risk Management Integrated Framework**, 2004'den aktaran I. Arslan, 2008, s. 28.
[92] **Etki**: Bir olayın olması durumunda riskin yaratacağı şiddetidir. **Olasılık**: Bir olayın gerçekleşme olasılığını belirtir.

strateji ile yönetileceğine karar verilmesidir. (Riskten kaçınmak, azaltmak, paylaşmak, kabul etmek) KRY süreci aşağıdaki şekilde gösterildiği gibi üç aşamadan oluşur.[93]



Şekil 7: Kurumsal Risk Yönetim Süreci

4.2. Risk İştahı ve Risk Toleransı

KRY'de birbirleriyle yakın anlam taşıyan risk iştahı, risk toleransı kavramlarının doğru anlaşılması büyük önem taşımaktadır.

Risk İştahı: Firmanın stratejik hedeflerini gerçekleştirirken almaya niyetli olduğu risk seviyesinin bir göstergesi olup, risk iştahının belirlenmesi stratejik bir karardır. Oldukça agresif bir politika veya yüksek risk alımıyla mı hareket edilecektir, yoksa söz konusu hedeflere ulaşılmaya çalışılırken aşılmaması gereken limitler mi belirlenecektir. Bu sorulara firma tarafından verilecek yanıtlar firmanın risk iştahının göstergesidir.

Örn: Kredi kartı pazarındaki piyasa payını arttırmaya çalışan bir bankanın kendisine başvuruda bulunan müşterilere uyguladığı araştırma kriterleri, risk iştahının bir göstergesidir. Sadece maaş belgesini yeterli gören ve kefil isteyen bir banka ile müşterinin

[93]Tamer Saka, Alper Uğural, **Kurumsal Risk Yönetimi**, 2014, s. 22, http://tusiad.org/tr/tum/item/download/2466_aff40c11210dd71986e25302c58160ca

kredi değerliliği hakkında detaylı araştırma yapan bir bankanın risk iştahları farklı olacaktır.[94]

Risk Toleransı: Firmanın hedeflerini gerçekleştirilmesi sırasında kabul edilebilecek dalgalanma, değişkenlik seviyesidir. Risk toleransı içerisinde faaliyet göstermek firmanın risk iştahı içerisinde kaldığına dair güvence verir ve firmanın hedeflerini gerçekleştireceğine dair daha yüksek derecede güvence sağlar.[95]

Örn: AQB tekstil firmasının kendisine girdi sağlayan tedarikçilerde kritik ürünlerde +-1 gün diğer ürünlerde +-3 gün gecikme olmasına izin vermesi veya zamanında teslim oranının %95'in altına düşmemesini istemesi, risk toleransını veya diğer bir deyişle katlanacak risklerin alt ve üst sınırını göstermektedir.[96]

Risk iştahı ise, risk toleransından daha geniş bir kavramdır. Risk toleransı taktiksel ve operasyoneldir. Risk toleransı, dört hedef kategorisinin tümüne uygulanır. (Stratejik, operasyonlar, raporlama ve uyumluluk) Risk toleransı kabul edilebilir sınırları belirler.[97]

Açık bir risk iştahı ifadesi olmadan, RY sürecinin hedefleri konusunda açıklık kazanmak mümkün değildir. Risk iştahının açıkça ifade edilmesi; yönetim kurulu üyelerinin, yöneticilerin ve çalışanların kabul edilebilir risk konusunda ortak bir görüş paylaşmalarını kolaylaştırır. Aynı zamanda kuruluşun her bir bölümünün genel risk yönetim stratejisine nasıl katkıda bulunduğunu gösterir. Strateji, RY ve risk iştahıyla iç içe geçmiş durumdadır ve bunlar birlikte düşünülmelidir. Etkili RY'nin temel taşı olarak açıkça ifade edilmiş bir risk iştahı aşağıdaki avantajları sağlayacaktır.[98]

---

[94] Ç. Özbek, 2012, s. 315.
[95] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. 18'den aktaran Ç. Özbek, 2012, s. 317.
[96] a.g.e.
[97] Larry Rittenberg, Frank Martens, **Understanding And Communicating Risk Appetite**, COSO Enterprise Risk Management, https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf
[98] Chartered Institute of Internal Auditors, **Risk Appetite And Internal Audit**, 2017, https://www.iia.org.uk/resources/risk-management/risk-appetite/

• RY'nin uygulanmasını yönlendiren bir başlangıç noktası oluşturur,

• RY içindeki stratejik hedeflere odaklanmayı sağlar,

• Risklere karşı nasıl cevap verilmesi gerektiğinin anlaşılmasını sağlar,

• Risklerin doğru bir şekilde tanımlanıp, yönetilip yönetilmediğini sorgulamak için bir temel oluşturur.

4.3. Kurumsal Risk Yönetiminde Rol ve Sorumluluklar

Bir işletmedeki herkes kurumsal risk için bir takım sorumluluklara sahiptir. İcra kurulu başkanı (CEO) nihai olarak risk yönetiminde sorumludur ve sahiplik etmelidir. Diğer yöneticiler RY felsefesini destekler, risk iştahına uyumluluğu teşvik eder ve risk toleranslarıyla tutarlı sorumluluk alanlarında riskleri yönetir. Yönetim kurulu, KRY'ye önemli ölçüde gözetim sağlar. Bir takım dış taraflarda genellikle KRY'ye fayda sağlamak için yararlı bilgi sağlar ancak kuruluşun KRY'nin etkinliğinden sorumlu değildirler. Yönetim kurulu, yönetim, risk görevlileri, mali sorumlular, iç denetçiler ve bir kuruluş içindeki herkes etkin KRY'ye katkıda bulunur.[99]

Üst Yönetim: Üst yönetim, KRY'de dahil olmak üzere bir işletmenin tüm faaliyetlerinden doğrudan sorumludur. Doğal olarak, farklı düzeydeki yönetim farklı KRY sorumluluklarına sahiptir. Bunlar, kurumun özelliklerine bağlı olarak genellikle önemli ölçüde değişir.[100]

[99] COSO, **Enterprise Risk Management - Integrated Framework**, Executive Summary, 2004, http://ehss.moe.gov.ir/getattachment/2b57139a-e934-4f59-84f9-c9b46e385241/, s. 83.
[100] a.g.e, s. 84.

Yönetim Kurulu: Yönetim kurulu, kurumun risk felsefesini anlamalı ve kurumun risk alma istekliliği konusunda yönetimle hem fikir olmalıdır. RY'nin etkin bir şekilde çalışıp çalışmadığını sorgulamalı, risk portföyünü gözden geçirmeli ve kurum risk alma isteklili-ğini sınırı ile karşılaştırmalıdır. Yönetim kurulu önemli riskler konusunda haberdar edil-meli ve yönetimin doğru tutumu sergileyip sergilemediğini değerlendirmelidir.[101]

Risk Görevlisi: Bazı şirketler, KRY'yi kolaylaştırmak için merkezi bir koordinasyon noktası oluşturmuştur. Bazı organizasyonlarda baş risk sorumlusu veya risk yöneticisi olarak anılan bir risk sorumlusu, sorumluluk alanlarında etkili RY oluşturmada diğer yöneticilerle birlikte çalışır. Risk yöneticisi, şirketin genel müdürlüğünün himayesinde kurulur ve bu risk altındaki kuruluşların, işletmelerin, departmanların, fonksiyonların ve faaliyetlerin KRY'ye yardımcı olacak kaynakları vardır. Risk sorumlusu ilerlemenin izlenmesinden ve diğer yöneticilere, ilgili risk bilgilerini yukarı, aşağı ve kuruluş genelinde rapor etmede yardımcı olmaktan sorumlu olabilir. Risk sorumlusu ek bir raporlama kanalı işlevi de görebilir.[102]

İç Denetim: Yönetim kurulu RY süreçlerinin etkinliğini değerlendirmek ve bu süreçlerin gelişmesine katkı sağlamak için iç denetçileri görevlendirebilir. İç denetçinin RY süreçlerinin faal olup olmadığına ilişkin tespiti, aşağıda sayılanların değerlendirilmesi sonucu varılan bir hükümdür:[103]

a) Kurum hedefleri misyonu destekler ve ona uyar.

b) Önemli riskler belirlenir ve değerlendirilir.

[101] D. Pehlivanlı, 2014, s. 175.
[102] COSO, **Executive Summary**, 2004, s. 86.
[103] COSO; Gleim Publications, **Control Framework And Fraud**, Study Unit Four, 2015,TİDE (Çev.), s. 10, https://www.gleim.com/

i) Riskleri ve kurumun risk iştahını birbirine uyumlu haline getiren uygun risk yanıtları seçilir.

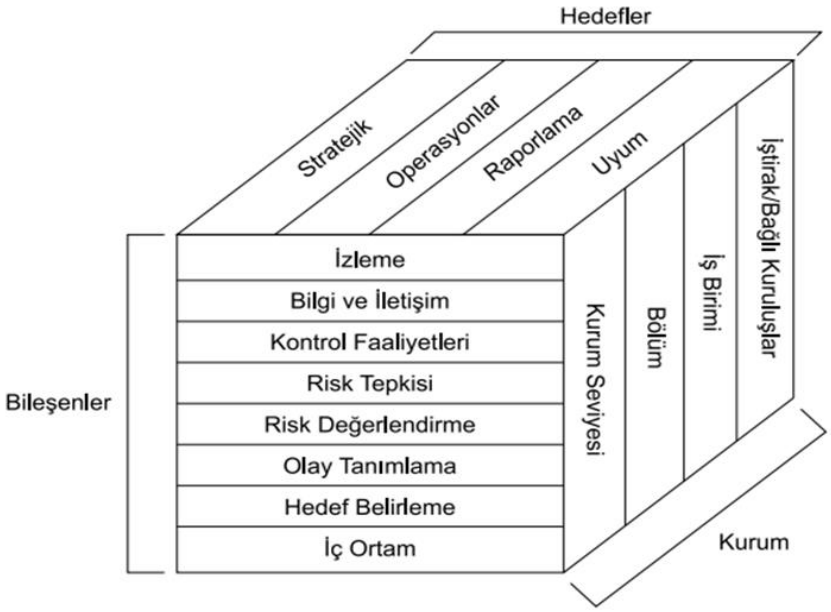
ii) İlgili risk bilgileri elde edilir ve kurumun tamamına zamanında iletilir ve böylece personelin, yönetimin ve yönetim kurulunun sorumluluklarını yerine getirmeleri sağlanır.

4.4. COSO Kurumsal Risk Yönetimi Modeli

KRY, uluslararası referans standartları kullanılarak uygulanabilmektedir. Bu noktada; işletmenin boyutu, riske bakış açısı, sektörel dinamikler ve RY'nin hangi olgunluk seviyesinde uygulamak istediği önem kazanmaktadır. KRY konusunda, özellikle yaşanan küresel krizlerin de etkisiyle, finansal veya finans dışı işletmeler tarafından artan bir ilgi mevcut olmakla birlikte, RY kavramının algılanışı açısından net bir konsensus bulunmamaktadır. Sigorta işletmeleri, bankalar, kredi kuruluşları, medikal endüstri vd. çeşitli sektörün kendine özgü risk yönetimi tanımlarının varlığı, günümüzde bile etkin bir RY stratejisinin tesisine yönelik genel geçer bir çerçeve veya standartın olmamasına neden olmaktadır. Bununla birlikte, KRY kavramının uluslararası olarak tanımının netleştirilmesine yardımcı olmak amacıyla 1990'lı yıllardan bu yana belli başlı standart ve çerçeveler yayınlanmış olup, bugün referans olarak kullanılan standartlar geliştirilmiştir.[104] 2004 yılında COSO tarafından yayınlanan ERM çerçevesi, uluslararası alanda kabul gören bir uygulama modeli olarak karşımıza çıkmaya başlamıştır.

[104] Bünyamin Topçu, İşletmelerde Kurumsal Risk Yönetimi, **İstanbul Ticaret Odası Yayınları**, 2012, http://www.ito.org.tr/itoyayin/0015264.pdf, S.27, s. 25.

Grafikle Gösterim: ‘‘COSO Kurumsal Risk Yönetimi Çerçevesi’’[105]; satırlar, kesitler ve sütunlardan oluşan küp biçimindeki bir matris olarak gösterilir. Satırlar sekiz bileşendir, kesitler dört hedef kategorisidir, sütunlar ise kurumun organizasyonel birimleridir. Kurum, çerçevenin her kesişim noktasında uygun yanıtı vermelidir. Örn: Bölüm düzeyinde raporlama hedeflerine ulaşmak için kontrol faaliyetleri gibi.[106]



Şekil 8: COSO Kurumsal Risk Yönetimi Çerçevesi

Kaynak: COSO; Gleim Publications, **Control Framework and Fraud**, Study Unit Four, 2015, TİDE (Çev.), s. 11, https://www.gleim.com

[105] Risk Yönetim Çerçevesi: Bir kurumun risk yönetim süreçlerini uygulamak için kullanmayı seçtiği yapılar, metodolojiler, prosedürler ve tanımların toplamı anlamına gelir. IIA, 2009, s. 8.
[106] COSO; Gleim Publications, **Control Framework and Fraud,** Study Unit Four, 2015, TİDE (Çev.), s. 11, https://www.gleim.com/

4.4.1. COSO Kurumsal Risk Yönetimi Modeli Bileşenleri

COSO KRY çerçevesi, birbiriyle ilişkili sekiz bileşenden oluşmaktadır. Bu bileşenler COSO KRY küpünde yatay kısımda yer alır. Bunlar: İç ortam, hedef belirleme, olay tanımlama, risk değerlendirmesi, risk tepkisi, kontrol faaliyetleri, bilgi/iletişim ve izleme'dir.

4.4.1.1. İç Ortam

COSO ERM'de iç ortamı şöyle tanımlamaktadır: ''İç ortam bir kurumun (genel havasını-the tone) oluşturur ve ERM'nin diğer tüm bileşenleri için temel bir yapı teşkil eder ve bu yapı disiplini sağlamaya yardımcı olur. İç ortam faktörleri; risk iştahı, yönetim kurulu tarafından sağlanan gözetim seviyesi, etik değerlerler, çalışanların yetkinliği ve yeterlilik seviyesi, organizasyon içinde yetki ve sorumluluk dağılımı gibi konulardır.'' İç ortam konusunda ERM iki ana konuya özellikle temas etmektedir.[107]

Birincisi, kurumun RY felsefesi ikincisi ise dürüstlük ve etik değerlere bağlılıktır. RY felsefesi, COSO ERM modelinde: ''Bir işletmenin risk yönetimi felsefesi temel stratejilerin oluşumundan söz konusu stratejilerin günlük operasyonlara uygulanmasına kadar karşılanan risklere nasıl reaksiyon verileceğini gösteren genel tavırlar ile paylaşılan değer yargılarının bir birleşimidir.'' şeklinde tarif edilmiştir. COSO ERM modelinde yukarıdaki ifade ile bahsedilmeye çalışılan husus, kurum içinde ne ölçüde bir risk farkındalığının olduğu, üst düzey yöneticilerden başlayarak tüm çalışanların günlük faaliyetlerini risk yönetiminin ne ölçüde hesaba veya süreçlere dahil edildiğidir. İkinci husus olan, dürüstlük ve etik değerler, ERM modelinde şu şekilde açıklanmaktadır:

[107] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. (5-9)'dan aktaran Ç. Özbek, 2012, s. 288-289.

‘‘ERM’nin etkinliği kurum faaliyetlerini yaratan yöneten ve izleyen çalışanların dürüstlük ve etik değerlerinin üstünde olmaz.’’[108]

4.4.1.2. Hedef Belirleme

COSO ERM modelinin ikinci bileşeni, RY sürecinin ilk aşaması olan kurum hedeflerinin belirlenmesidir. Her kurum çeşitli muhtelif risklerle karşılaşır, karşılaşılan risklerin belirlenmesi ve değerlendirilmesinden önce kurumun hedeflerinin belirlenmesi gerekir. Bir kurumun hedeflerinin belirlenmesi stratejik hedeflerin belirlenmesi ile başlar ve bunun için ilk aşama stratejik bir vizyonun belirlenmesidir. COSO ERM, hedeflerinin belirlenmesini şu adımlarla özetlenmektedir:[109]

- **Misyon/Vizyon--Ana Stratejik Hedefler--Stratejiler--İlgili Hedefler**

4.4.1.3. Olay Tanımlama

Olay tanımlama aşaması, bir önceki adımda belirlenen kurum hedeflerinin gerçekleştirilmesini olumlu etkileyebilecek fırsatların veya olumsuz etkileyebilecek tehditlerin (risklerin) diğer bir deyişle firmanın hedeflerini gerçekleştirmesini olumlu veya olumsuz etkileyebilecek tüm ‘‘Olay’’ların tanımlanması aşamasıdır. Belirsizlikler işletmeler için olumsuz sonuçlar ortaya çıkarabileceği gibi fırsatları da meydana getirebilmektedir. Olay tanımlama bileşeninde risk yerine olay kelimesinin kullanılmasının nedeni, belirsizliklerin yaratacağı hem tehditlerin hem de olası fırsatların tanımlanmasıdır.[110]

---

[108] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. (5-9)’dan aktaran Ç. Özbek, 2012, s. 288-289.
[109] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. (13-14)’den aktaran Ç. Özbek, 2012, s. 299.
[110] Ç. Özbek, 2012, s. 317.

COSO ERM modelinde olay tanımlaması adımı şu şekilde açıklanmıştır: ‘‘Yönetim gerçekleşmesi muhtemel (olumlu veya olumsuz yönde) olası olayları tanımlar ve bu olayların bir fırsat yaratıp yaratmayacağını belirler. Olumsuz olaylar genellikle riskleri temsil eder. Olumlu olaylar ise fırsatları işaret etmektedir.’’[111]

4.4.1.4. Risk Değerlendirme

COSO ERM risk değerlendirmesi bileşenini şu şekilde açıklamaktadır: ‘‘ Risk değerlendirme işletmenin hedeflerinin gerçekleştirilmesi üzerinde hangi olası olayların ne ölçüde etkili olacağını göz önünde bulundurmaları konusunda yol gösterir. Yönetim risklerin değerlendirilmesinde nicel veya nitel yöntemler kullanabilir. Olumlu ve olumsuz olaylar risk bazında ve kurum çapında değerlendirilir. Riskler (doğal ve kalıntı risk)[112] olarak değerlendirmeye tabi tutulur.’’[113]

Risk etki ve olasılık cinsinden ölçülür. (Risk=Etki x Olasılık) ve bu değerlendirme bir matris üzerinden puanlanarak risklere nasıl yanıt verileceğine karar verilir.

4.4.1.5. Risk Tepkisi

Bu aşamada risklere verilebilecek cevaplar belirlenir ve değerlendirir. Bu bağlamda, risklere verilebilecek tepki dört şekilde gerçekleşebilir:[114]

Riskten Kaçınma: Yapılacak faaliyetten vazgeçmek anlamına gelir.

Riski Azaltma: Riskin etki ve olasılıklarını azaltmaya yönelik faaliyetleri tanımlar.

Riski Paylaşma: Riski transfer etme veya bir bölümünü paylaşmak anlamına gelir.

Riski Kabul Etme: Riske karşı hiçbir aksiyonda bulunulmaması demektir.

---

[111] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. 18’den aktaran Ç. Özbek, 2012, s. 317-318.

[112] Geniş bilgi için bkz. Bölüm*:* (5.2.1).

[113] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. (33-53)’den aktaran Ç. Özbek, 2012, s. 346.

[114] Ş. Güneş, 2009, s. 33.

4.4.1.6. Kontrol Faaliyetleri

Kontrol faaliyetleri, yönetimin risk yanıtlarının gerçekleştirilmesini sağlayan politikalar ve prosedürlerdir. Kontrol faaliyetleri, organizasyonun her kademesinde ve tüm işlevlerde gerçekleşir. Onaylar, yetkilendirmeler, doğrulamalar, işletme performansının gözden geçirilmesi, varlıkların güvenliği ve görevlerin ayrılması kadar çeşitli faaliyetler içerirler. Kontrol faaliyetleri, yönetimin risk yanıtlarının gerçekleştirilmesini sağlamak için doğrudan veya teknolojinin uygulanması yoluyla politikaları uygulamak için insanların eylemleri olan politikalar ve prosedürlerdir.[115]

4.4.1.7. Bilgi ve İletişim

Bilgiler, kişilerin sorumluluklarını yerine getirmelerini sağlayan biçim ve zaman çerçevesinde tanımlanır, elde edilir ve iletilir. Bilgi sistemleri, kurum içi üretilen verileri ve dış kaynaklardan gelen bilgileri kullanarak, riskleri yönetmek ve bilgilendirilmek üzere bilgi sağlar. Tüm personel, üst düzey yönetimden KRY sorumluluklarının ciddiye alınması gerektiğine dair açık bir mesaj alır, kurumsal risk yönetimindeki kendi rollerini ve bireysel faaliyetlerin, başkalarının işi ile nasıl ilişkili olduğunu anlarlar. Müşteriler, tedarikçiler, düzenleyiciler ve hissedarlar gibi dış taraflar arasında etkili bir iletişim vardır.[116]

[115] COSO, **Enterprise Risk Management - Integrated Framework**, Executive Summary, 2004, http://ehss.moe.gov.ir/getattachment/2b57139a-e934-4f59-84f9-c9b46e385241/, s. 61.
[116] COSO, **Enterprise Risk Management - Integrated Framework**, Executive Summary, 2004, s. 67.

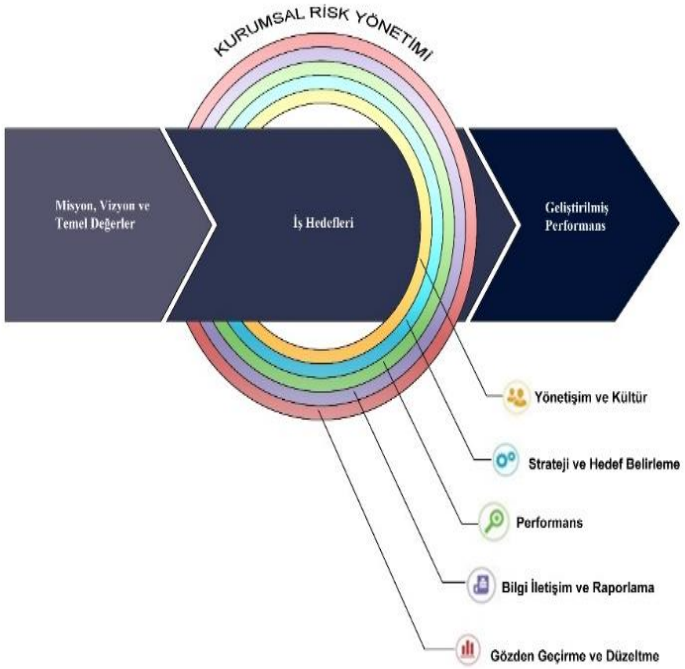
4.4.1.8. İzleme

Kurumlar risk yönetimini izlerler ve zaman içinde bileşenlerinin varlığını ve işleyişini değerlendirirler. İzleme faaliyeti; sürekli izleme faaliyetleri, ayrı değerlendirmeler veya ikisinin bir kombinasyonu ile gerçekleştirilebilir. Ayrı değerlendirmelerin kapsamı ve sıklığı öncelikle risklerin değerlendirilmesine ve devam eden izleme prosedürlerinin etkinliğine bağlı olacaktır. Kurum çalışanlarının RY eksikliklerini ve ciddi konuları üst yönetim ve yönetim kuruluna bildirilmesi gerekir.[117]

4.5. COSO KRY Riskin Strateji ve Performansla Uyumlaştırılması Modeli

COSO tarafından yayınlanan üç rapor vardır: Birincisi 1992 yılında yayınlanan ve 2013 yılında revize edilen ‘‘İç Kontrol Entegre Çerçevesi’’ ikincisi ise, 2004 yılında geliştirilen “Kurumsal Risk Yönetimi Entegre Çerçevesi”dir. Üçüncüsü, 6 Eylül 2017 tarihinde “Kurumsal Risk Yönetimi Riskin Strateji ve Performansla Uyumlaştırılması” adıyla KRY’den revize edilmiş ancak farklı bir uygulama modeli olarak yayınlanmıştır.[118] Yenileme ile çerçevenin adı ve yapısı da değiştirilmiştir. Çerçevenin adında, strateji, risk ve performans arasındaki ilişkiye vurgu yapılmıştır. Yeni çerçevede 5 adet bileşen (Yönetişim&Kültür, Strateji&Hedef Oluşturma, Performans, Gözden Geçirme&Düzeltme, Bilgi, İletişim&Raporlama) ve bunlara ilişkin 20 adet prensip belirlenmiştir.[119]

[117] COSO, **Enterprise Risk Management - Integrated Framework**, Executive Summary, 2004, s. 75.
[118] Nazif Burca, **Yenilenen COSO Kurumsal Risk Yönetimi Çerçevesi**, 2017, https://nazifburca.com/2017/09/20/yenilenen-coso-kurumsal-risk-yonetimi-cercevesi/
[119] N. Burca, 2017.



Şekil 9: COSO KRY Riskin Strateji ve Performansla Uyumlaştırılması Modeli

Kaynak: https://commsrisk.com/new-coso-erm-framework-out-for-comment/

Çerçeve birbiriyle ilişkili beş bileşen halinde düzenlenen bir dizi ilkeden oluşmaktadır. Bileşenler aşağıdaki gibidir:[120]

1. Yönetişim ve Kültür: Yönetişim, örgütün tonunu belirler. KRY için önemi; gözetim sorumluluklarının oluşturulması, kültür, etik değerler, arzulanan davranışlar ve riskin anlaşılmasına ilişkindir.

2. Strateji ve Hedef Belirleme: KRY; strateji ve hedef belirleme, stratejik planlama sürecinde birlikte çalışır.

3. Performans: Stratejinin ve işin başarısını etkileyebilecek risklerin, hedeflerin tanımlanması ve değerlendirilmesi gerekmektedir.

[120] COSO, **Enterprise Risk Management Integrating With Strategy and Performance**, Executive Summary, 2017, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

4. Gözden Geçirme: Bir kuruluşun performansını gözden geçirerek, KRY bileşenleri zaman içinde ne kadar iyi çalışıyor ve önemli değişiklikler olduğunda hangi revizyonlara ihtiyaç duyulduğunun belirlenmesi gerekir.

5. Bilgi, İletişim ve Raporlama: KRY gerekli bilgiyi elde etme ve paylaşma sürecini sürekli gerektirir.

COSO 2004 çerçevesinde KRY*:* "Bir kurumun yönetim kurulu, yöneticileri ve tüm çalışanlarından etkilenen, stratejinin belirlenmesinde ve kurum genelinde uygulanan, kurumu etkileme potansiyeli olan olayları belirleme ve risk iştahı çerçevesinde riskin yönetilmesi amacıyla dizayn edilen, kurumun hedeflerini başarması için makul güvence sağlayan bir süreçtir." şeklinde tanımlanmıştır. Güncellenen çerçevede ise KRY: "Organizasyonun değer yaratma, koruma ve realize etmede, riski yönetmek için güvenebilecekleri, stratejinin belirlenmesi ve yürütülmesine entegre edilen, kültür, imkân ve uygulamalardır." şeklinde tanımlanmıştır. KRY'nin statik olmadığı, günlük alınan kararlar vasıtasıyla, strateji geliştirme, iş hedeflerinin oluşturulması ve bu hedeflerin uygulanmasına entegre olduğu belirtilmiştir. Unsurlar ve bunlara ilişkin prensiplerin belirlenmesi, çerçevenin kullanım kolaylığı ve daha iyi anlaşılması bakımından uygun olmuştur. Küp şeklinde gösterimden vazgeçilmesi, COSO iç kontrol küpü ile karıştırılmasını önlemek ve kurumsal risk yönetimin kurumun tüm süreçlerine entegre olduğunu göstermek açısından faydalı olmuştur, çerçevede yer alan "Kontrol Faaliyetleri" bileşeni bu çerçevede belirtilmemiş, ancak ''COSO İç Kontrol Çerçevesine'' atıf yapılarak kontrol faaliyetleri hakkında bu çerçevenin halen geçerli olduğu ifade edilmiştir.[121]

[121] N. Burca, 2017.

Yenilenen COSO ERM yeni bir yapı getirmiştir. Yönetişimden gündelik faaliyetlere kadar olan süreçleri kapsamaktadır. Büyüklüğü, türü veya sektöre bakılmaksızın tüm organizasyonlara uygulanabilir niteliktedir ve yönetim kurulu ve yönetim arasındaki risk hakkında daha zorlu bir iletişime izin vermektedir. Risk yönetiminin entegrasyonu üzerinde odaklanmayı sağlamaktadır: Çerçeve; risklerin strateji belirleme ve günlük faaliyetlerle ilişkilendirilmesi, bir organizasyonun kültürüne, yeteneklerine ve uygulamalarına götürülmesine ve daha iyi karar verme mekanizmalarının geliştirilmesine yardımcı olmak için KRY'nin daha iyi nasıl entegre edileceği konusunda rehberlik etmektedir. İşletme perspektifinden yazılmıştır. Kültürün daha fazla vurgulanmasını içerir. Çerçeve, KRY uygulamalarının, bir organizasyonun kültürüne daha fazla şeffaflık ve risk bilinci oluşturmasını ve bu kararların şekillendirilmesinde kültürün önemini kavrayarak insanların karar vermelerine yardımcı olmasını ele almaktadır. Bilgi teknolojisinin değişen rolünü de inceleyerek verilerin çoğalması, yapay zekâ ve otomasyon gibi iş eğilimlerine ışık tutmaktadır.[122]

Yenilenen COSO ERM'de en önemli değişikliklerin bazıları aşağıda özetlenmiştir. Güncellenmiş belge aşağıdaki özellikleri içermektedir:[123]

• Bileşen ve ilkeler yapısını benimsemektedir.

• KRY tanımını basitleştirmiştir. Güncellenmiş belgede KRY tanımı, daha unutulmaz ve okunabilir hale getirilmek üzere yeniden düzenlenmiştir, Örneğin, riskin tanımı strateji ve hedeflerin başarılmasıyla ilişkilidir.

• Risk ve değer arasındaki ilişkiyi vurgulamaktadır.

• KRY'nin entegrasyonu üzerine odaklanmayı yenilemektedir.

[122] Dennis Chesley, pwc, **The Top Changes To The COSO ERM Framework You Need To Know Now**, 2017, http://pwc.blogs.com/resilience/2017/09/the-top-changes-to-the-coso-erm-framework-you-need-to-know-now.html

[123] COSO, **Enterprise Risk Management Integrating With Strategy and Performance**, June 2017, Frequently Asked Questions, https://www.coso.org/Documents/COSO-ERM-FAQ-September-2017.pdf

• Kültür rolünü incelemektedir, kültürün KRY uygulamaları üzerindeki etkisinin önemi, güncellenmiş belgede tanıtılan ilk kavramlardan biridir.

• Strateji tartışmalarını artırmaktadır.

• Performans ve KRY arasındaki uyumu artırmaktadır.

• KRY'yi daha açık bir şekilde karar alma sürecine bağlamaktadır.

• KRY ve İK arasındaki ilişkiyi belirtmiştir.

• Risk iştahını ve toleransını düzenlemiştir.

Güncellenmiş tanım, riski değer kavramıyla daha yakından uyumlaştırılmaktadır. Risk tanımını iyileştirmekte ve strateji ve performans tartışmalarını artırırken, KRY'nin değeri yaratmada, korumada ve gerçekleştirmede oynadığı rolü vurgulamaktadır. KRY'nin strateji belirleme sürecine entegrasyonu, işletme hedeflerinin belirlenmesi ve yürütülmekte olan riskin yönetilmesi ile başlar ancak risk değerlendirmesi ek veya ayrı bir faaliyet olarak konumlandırılmamaktadır. Güncellenmiş belge, risk raporlamasına değil, bunun yerine performansı etkileyen potansiyel veya gerçek risk teşhisine ve strateji ve işletme hedeflerine ulaşılmasına ilişkin raporlar üzerinde durmaktadır.[124]

[124] COSO, **Executive Summary**, 2017.

BEŞİNCİ BÖLÜM

RİSKLERİN YÖNETİLMESİ VE KONTROLÜNDE KAVRAMSAL İLİŞKİLER

5.1. Risk Yönetimi, Risk Değerlendirme ve Risk Analizi İlişkisi

RY, IIA'nın tanımında: ''Kurumun amaçlarını gerçekleştirmek üzere makul bir güvence sağlamak amacıyla potansiyel olay ve durumları belirleme, değerlendirme yönetme ve kontrol etme süreci şeklinde açıklanmıştır.''[125] RY; risklerin tanımlanması, değerlendirilmesi, risklerin giderilmesi (cevap verilmesi) ve izlenmesinden oluşan genel bir süreçtir. COSO'ya göre risk değerlendirmesi ise bir RY süreci adımı olmakla birlikte İK bileşenlerinde de yer alır.

Aşağıda belirtilen ''COSO İç Kontrol Çerçevesi'' prensiplerinden dört tanesi risk değerlendirme adımına aittir:[126]

• **Prensip 6**: Kurum, hedeflerini ve söz konusu hedeflere yönelik risklerin tanımlanması ve değerlendirilmesini sağlayacak yeterli nitelikte belirler.

• **Prensip 7**: Kurum, hedeflerinin gerçekleştirilmesine yönelik riskleri kurum çapında tanımlar ve risklerin nasıl yönetileceğine bir temel teşkil etmek üzere söz konusu riskleri analiz eder.

• **Prensip 8**: Kurum, hedeflerinin gerçekleştirilmesine yönelik risklerin değerlendirilmesinde usulsüzlük olasılığını göz önünde bulundurur.

• **Prensip 9**: Kurum, İKS'yi önemli derecede etkileyebilecek değişikleri tanımlar ve değerlendirir.

---

[125] IIA, **Standartlar**, UMUÇ, 2017, s. 28.

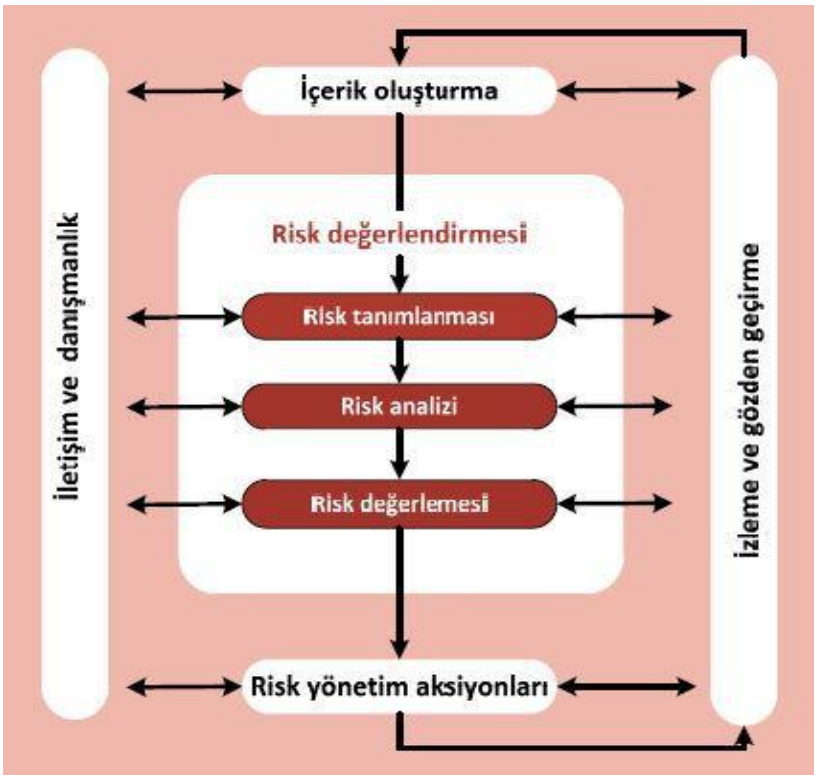
[126] COSO, **Internal Control - Integrated Framework**, Framework and Appendices, Risk Assesment, 2012, http://aechile.cl/wp-content/uploads/2012/11/coso_framework_body1.pdf, s. 13.

‘‘COSO İç kontrol Bütünleşik Çerçevesi’’ 7. prensibe baktığımızda risk değerlendirmesini aşağıdaki sorulara cevap aramaktadır:[127]

(1) Kuruluşun hedeflerine ulaşmasının önündeki riskler nelerdir?

(2) Belirli bir riskin oluşması ihtimali nedir ve olursa ne kadar şiddetli olabilir ve bu risk şirketi ne kadar sürede etkileyecek ve ne kadar sürecek?

(3) Bir olay olması durumunda yönetim nasıl yanıt vermelidir? Dört yanıt türü vardır: (Kabul, kaçınma, azaltma ve paylaşma)



Şekil 10: ISO 31000 Risk Yönetim Süreci

Kaynak: https://www.theirm.org/media/1001360/SARMERMPublishFinal14Feb2012.pdf

[127] Warren W. Stippich, **The 4 Risk Assessment Principles of The 2013 COSO Framework**, Principle 7: Identify and Analyze Risks Across the Entity, 2015, http://www.corporatecomplianceinsights.com/the-4-risk-assessment-principles-of-the-coso-framework/

(ISO 31000)[128] RY sürecinde ise, risk değerlendirmesi ise aşağıda açıklanan üç adımdan oluşmaktadır:[129]

1) Risklerin Tanımlanması: İşletmeler; risk kaynaklarını, etki alanları, olayları (durum değişiklikleri dahil) ve bunların nedenlerini ve potansiyel sonuçlarını belirlemelidir. Bu adımın amacı; hedeflerin başarılmasını sağlayacak, geliştirecek, hızlandırabilecek veya erteleyebilecek olaylara dayanan kapsamlı bir riskler listesi oluşturmaktır.

2) Risklerin Analizi: Risk analizi, riskin anlaşılmasını içerir. Risk analizi, risk değerlendirmesine ve risklerin ele alınması gerekip gerekmediğine ilişkin kararlara ve en uygun risk tedavi stratejileri ve yöntemlerine girdi sağlar. Risk analizi, risklerin oluşma nedenlerini ve kaynaklarını, bunların olumlu ve olumsuz sonuçlarının ve bu sonuçların ortaya çıkma ihtimalinin dikkate alınmasını içerir. Bir olayın birden fazla sonucu olabilir ve birden çok hedefi etkileyebilir. Mevcut kontroller ve bunların etkililiğini ve etkinliği de dikkate alınmalıdır. Analiz, koşullara bağlı olarak (nitel ve nicel)[130] veya bunların bir kombinasyonu olabilir.

3) Risklerin Değerlemesi: Risk değerlemesinin amacı, risk analizinin sonuçlarına dayanarak, hangi risklerin tedaviye ihtiyacı olduğu ve tedavi uygulanmasının önceliği üzerine kararlar vermeye yardımcı olmaktır. Risk değerlendirmesi, analiz süreci sırasında bulu-

[128] **ISO 31000**: RY ile ilgili ISO kurumu tarafından basılmış yayınlanmış uluslararası bir standarttır. ISO 31000:2009 güncel versiyonudur. Standardın amacı, RY ile ilgili genel metodoloji ve kuralları sağlamaktır. ISO 31000 standardı, uygulayıcıları bölgesel ve ülkesel risk faktörlerinin belirli bir standart dahilinde değerlendirmek istemesinden orta çıkan bir standarttır. http://www.eurocert.com.tr/iso-31000-risk-yonetimi.aspx

[129] ISO, **Principles and Guidelines**, ISO 31000 Risk Management, First Edition 2009-11-15, http://ehss.moe.gov.ir/getattachment/56171e8f-2942-4cc6-8957-359f14963d7b/ISO-31000, s. 18.

[130] Risk analizi yöntemleri nitel ve nicel olmak üzere ikiye ayrılır. **Nitel Risk Analizi**: Gözleme dayalıdır, sayısal olarak ölçülemeyen özelliklere ilişkin araştırmaları kapsar. **Nicel Risk Analizi**: Rakamların ön plana çıktığı sonuçların istatistiksel olarak değerlendirildiği ve analiz edildiği yöntemleri kapsamaktadır. https://ipfs.io/ipfs/QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Risk_analizi.html

nan risk düzeyini, oluşturulan risk ölçütleriyle karşılaştırmayı içermektedir. Bu karşılaştırmaya dayanarak, tedaviye olan ihtiyaç göz önüne alınabilir. Kararlar, riskin daha geniş bağlamını hesaba katmalı ve bunun toleransını dikkate almalıdır.

5.2. Risk Yönetimi ve Risklerin Kontrolü

RY ve risk kontrolü kavramlarını iyi anlamak için öncelikle kontrol kavramına odaklanmak gerekir. IIA kontrolü şöyle tanımlamıştır: ‘‘Kontrol, yönetimin denetim kurulunun, yönetim kurulunun ve diğer uygun birimlerin riski yönetmek ve belirlenen amaç ve hedeflere ulaşma ihtimalini artırmak amacıyla aldığı tedbirlerdir. Yönetim, hedef ve amaçların gerçekleştirilmesine yönelik makul bir güvence sağlamak için yeterli tedbirin alınmasını planlar, tertipler ve yönlendirir.’’[131]

Ülkemizde özellikle denetim terminolojisinde kontrol kavramı ile bir işlemin gerçekleştirilmesinden veya tamamlanmasından sonra söz konusu işlemin doğru veya mevzuata uygun gerçekleşip gerçekleşmediğinden bizzat kontrol etmekle yükümlü (denetçi) bir görevli tarafından kontrol edilmesi anlaşılırken; uluslararası anlamda kontrol kavramı daha yönetsel bir içerik taşımakta belirli bir işlemin tamamlanmasından sonra değil aksine gerçekleşmesi sırasındaki yol ve yöntemleri de kapsayan süreçlerin içine yedirilmiş sürekli devam eden sorumluluğu sadece denetçiler üzerine yüklenmeyen aksine tüm çalışanların sorumluluk taşıdığı bir uygulama olarak karşımıza çıkmaktadır.[132]

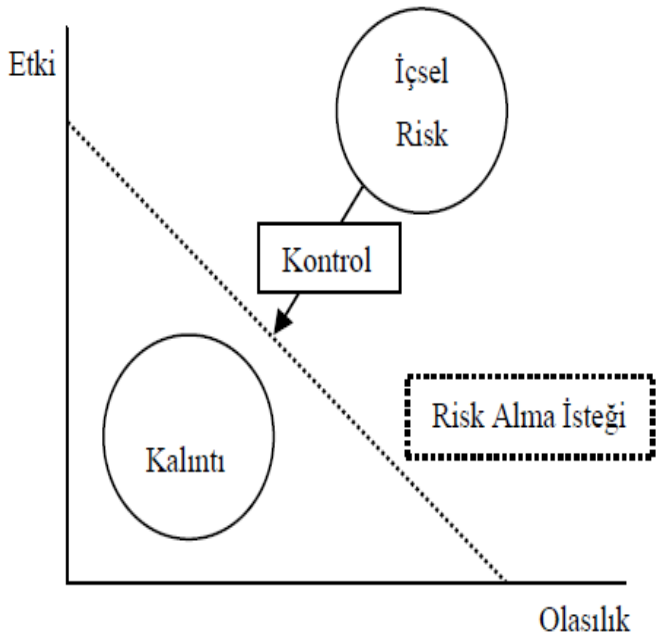
İK kavramı kaynaklarda genellikle kontrol kelimesi yerine kullanılır. Risklere yönelik bir süreç içerisinde uygulanan kontroller; tespit edici, telafi edici, düzeltici, önleyici kontroller olarak sıralanabilir. Bunun haricinde çeşitli kontrol faaliyeti

[131] IIA, **Standartlar**, UMUÇ, 2017, s. 27.
[132] Ç. Özbek, 2012, s. 385.

yöntemleri vardır. (Bilgi teknolojileri kontrolleri, görev ve sorumlulukların ayrıştırılması, fiziksel kontroller, bilgi işlem kontrolleri vd.)

5.2.1. Risk ve Kontrol İlişkisi

Bir işletmede hedefler, riskler ve kontroller birbirlerinin tamamlayıcısı durumundadır. İşletmeler belirli hedefler belirlerler ve bu hedeflerini sekteye uğratacak olumsuz durumların etki ve olasılıklarını azaltmak amacıyla çeşitli kontroller geliştirir ve uygularlar. Risklerin hedefler doğrultusunda belirlenmesi gerekir ve uygulanan kontrollerde risklere göre tasarlanmak zorundadır. Kurumlar hedeflerine ulaşmada engel teşkil edecek riskleri tanımlarlar, değerlendirirler ve risk iştahları doğrultusunda bu risklerin etki ve olasılıklarını hafifletmeye yönelik kontrolleri devreye sokarlar. Bu kontroller mevcut riskin şiddetini; içsel risk seviyesinden kalıntı risk seviyesine indirir.



Şekil 11: Risk Yönetimi İçerisinde Kontrollerin Yeri

Kaynak: David Griffith, **Risk Based Internal Auditing**, Versiyon 2. 2, http://www.internalaudit.biz/, s. 5.

Riski yönetmek ve belirlenmiş hedeflere ulaşma olasılığını artırmak amacıyla; yönetim, yönetim kurulu ve diğer taraflarca alınan herhangi bir tutum olarak tanımlanan kontrolün tanımında da belirtildiği üzere kontrol ve risk birbiriyle ilişkilidir.[133]

Risklerle ilgili anlaşılması gereken önemli bir husus; doğal veya içsel ve (artık risk)[134] kavramlarıdır. Doğal risk, sürecin doğasında yer alan ve bu riskin azaltılması için herhangi bir kontrol faaliyetinin olmaması halinde riskin oluşturabileceği zararı ifade etmektedir. Örneğin; yoğun yağış alması halinde sel tehlikesine uğrama ihtimali olan bir dere yatağına inşa edilen bir üretim tesisi açısından, olası bir sel baskınının vereceği zararın giderilmesine yönelik herhangi bir önlemin alınmadığı durumda meydana gelecek olan zarar, firmanın maruz kalacağı doğal riski ifade etmektedir. Çünkü bünyesinde herhangi bir kontrol önlemi içermemektedir. Ancak olası bir sel baskınına karşı, fiziksel koruma önlemlerinin alınması örneğin üretim tesisinin göreceli olarak yükseltilmiş bir alana yapılması, sel sularının gelebileceği alanlara yönelik duvarlar veya bariyerler konulması, sel baskınına karşı sigorta yapılması, söz konusu riske yönelik kontrol eylemleridir. Tüm alınan önlemlere rağmen söz konusu riskin gerçekleşmesi halinde oluşacak risk ise artık risktir.[135]

5.2.2. Risk Yönetimi/Kurumsal Risk Yönetimi ve İç Kontrol İlişkisi

RY; risklerin belirlendiği, analiz edildiği, risklere yönelik aksiyonların alındığı bir süreci kapsar. RY risk kontrolünü de içine alan geniş bir kavramdır. Dünya genelinde birçok iç kontrol çerçevesi veya standardı bulunmaktadır. ‘‘COSO İç Kontrol Bütünleşik

[133] IIA, **Yönetişim: Risk ve Kontrol ile İlişki**, UMUÇ, Uygulama Önerisi 2110: 2, Nisan 2010, TİDE (Çev.), https://www.tide.org.tr/

[134] IIA tarafından yenilenen UMUÇ’da, standartlarda yer alan terimler sözlüğünden, artık (kalıntı) risk kaldırılmıştır.

[135] Ç. Özbek, 2012, s. 238.

Çerçevesi'' bunlardan en yaygın olanıdır. Bu çalışmadaki kavramlar ''COSO İç Kontrol Bütünleşik Çerçevesi'' kapsamında, IIA standartları ve bakış açısıyla incelenmiştir.

RY ile ilişkisi bakımından İKS, risk yönetim sisteminin temeli olarak kabul edilebilir. İKS, yönetime işletme faaliyetlerinin doğasında var olan risklere karşı bu risklerin kontrolü ve yönetimi konusunda destek vermektedir.[136] RY, esasen iç kontrolü de kapsayan, daha geniş kapsamlı, daha stratejik ve daha zahmetli bir süreçtir. İç kontrolde üst yönetim, İK ile ilgili sorumluluklarını delege edebilmekte ve aktif katılım sağlayabilmektedir. Ancak risk yönetiminde, üst yönetimin sorumlulukları son derece yüksektir. Sadece destek vermek, oluşturulmasını sağlamak ve gözetim bağlamında düzenli rapor almak yetmemekte, risk yönetimine aktif katılım sağlanması ve risk gözetiminin çok daha sık gerçekleştirilmesi gerekmektedir.[137]

İK, KRY'nin önemli bir parçasıdır. İkisi birlikte kullanıldıklarında, yönetimi desteklemede güçlü tamamlayıcılar olurlar. İK, kuruluşların uyumluluk, raporlama ve operasyon hedeflerine ulaşmasına yardımcı olmak için tasarlanmış faaliyetleri içerir. Yönetimin ulaşmaya çalıştığı hedefler için riskleri göz önünde bulundurması gerekir. Bu nedenle, doğal olarak İK RY'nin bir bileşenidir. Ancak iç kontrolde ERM'yi tamamlar, her biri, diğerinin değerini yükseltir. Örn: ERM, kontrollerin geliştirilmesi için temel olarak kullanılan objektifin geliştirilmesine yardımcı olurken, İK, ERM'yi kontrol faaliyetleri, risk tepkileri ve diğer ERM süreçleri üzerinde uyguladığında daha etkili hale getirir.[138]

---

[136] David Galloway, **Internal Auditing: A Guide For The New Auditor**'den aktaran D. Pehlivanlı, s. 38.

[137] Bertan Kaya, **İşe Nereden Başlamalı: İç Denetim İç Kontrol veya Risk Yönetimi**, 2011, http://bertankaya.net/?p=498

[138] Dennis Chesley, Jason Pett, Frank Martens, **Powerful Complements: The Value of ERM And Internal Control Together**, http://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/publications/value-of-erm-and-internal-control-together.html

RY ve İK, birlikte sıklıkla bahsedilen kavramlardır. Kavramlar genellikle birbirlerine çok dar ve ayrı olarak algılanırlar. RY, spesifik kontrol faaliyetleriyle sınırlı değildir. İki kavram karşılaştırıldığında ikisi arasında yüksek oranda örtüşme olduğunu görülür. İK, ERM'nin bir sonucu ya da bir alt işlemi olarak görülebilir. Bu alt süreç, yönetim ve kontrol mekanizmalarının toplamı olarak tanımlanabilir. ERM, sadece belli bir anda şirketin statüsünü değil, gelecekteki olumlu ve olumsuz gelişmeleri de bütünsel bir perspektifle ele almak demektir.[139]

İç kontrolü arabayı kullanmak, risk yönetimini yol koşullarını izlemek olarak da örneklendirebiliriz. İki kavram iç içedir. Bir işletme başarılı olmak istiyorsa, her ikisini de yapmak zorundadır, buda başarılı olmasına katkı sağlayacaktır. KRY kavramı iç kontrolü terk etmek anlamına gelmemektedir. COSO komitesinin belirtiği gibi İK, KRY'nin ayrılmaz bir parçasıdır. İK, konvansiyonel (alışılagelmiş, geleneksel) riski çözmek için uğraşır. RY, rutin olmayan riski ortadan kaldırmayı amaçlar. RY; risk planlaması, risk kontrolü ve risk tepkisini içerir. Bu üç kavram birlikte tam bir risk yönetimi süreci oluşturur. Bunlardan risk kontrolü; dış ve İK olarak ayrılır. İK, bir iç risk kontrol mekanizmasıdır. İK, risk yönetiminden farklıdır. RY için temel görev risk planını oluşturmaktır. Risk kontrolü, risk planı kapsamında çeşitli kontrol faaliyetleri yürütür. Risk kontrolü, iç risk kontrolü (iç kontrol) ve dış risk kontrolünü içerir.[140]

[139] IIA Norge (Norveç), **Guidelines For The Risk Management Function**, 2017, http://iia.no/wp-content/uploads/2017/05/2017-Guidance-for-the-Risk-Management-Function.pdf, s. 7.

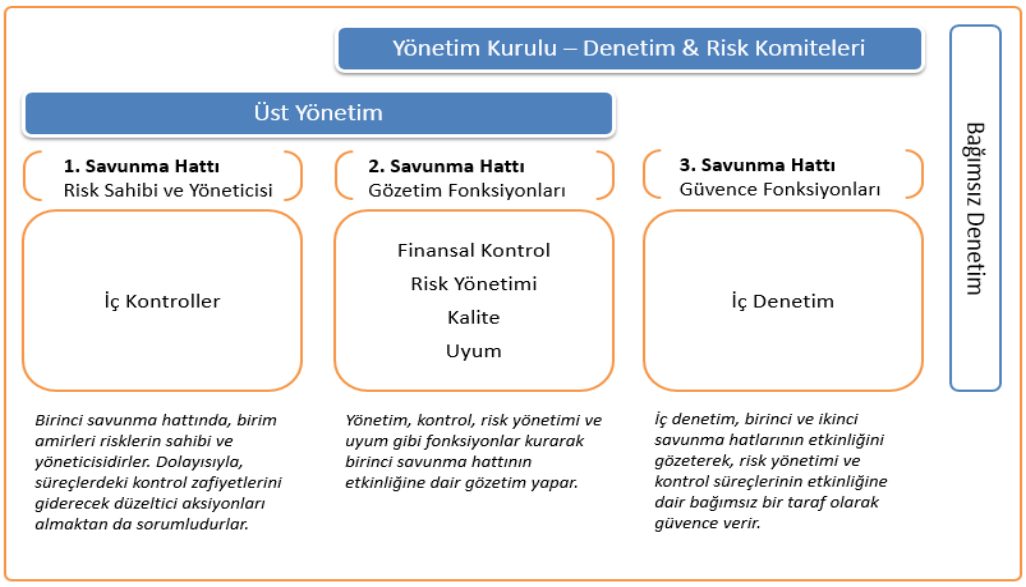
[140] Yan WU, **Enterprise Internal Control From The Perspective of Risk Management**, Jilin Business and Technology College, Changchun City Jilin Province, China, 2015, http://download.atlantis-press.com/php/download_paper.php?id=7314, s. 705.

5.2.3. Risk Yönetimi ve Kontrolünde Üç Savunma Hattı

Çeşitli örgütsel işlevlerin rol ve sorumluluklarını açıkça tanımlamak önemlidir. Bu kaynakların verimli kullanılmasına, tüm faaliyetler üzerinde tatmin edici bir kontrol seviyesine, görev ve işlevlerin çoğaltılmasından kaçınmasına (risk yönetimine ve iç kontrole bağlı faaliyetler dahil) katkıda bulunur. Bu aynı zamanda, işlevler arasındaki ara birimleri ve bunların organizasyonun genel RY ve İK yapısındaki konumlarını açıklığa kavuşturmayı da içerir. ‘‘Üç Hattın Savunması’’ modeli İK ve RY için rol ve sorumlulukların yüksek seviyede gözden geçirilmesini sağlar. Örgütlerde resmi bir risk yönetimi çerçevesi yada sistem bulunmayan organizasyonlarda bile, bu model organizasyonun ERM’sinin ve iç kontrolün anlaşılmasının geliştirilmesine yardımcı olabilir.[141]

İD, kurumsal yönetişim yapısında etkin bir RY sağlamak için önemli bir role sahiptir. Yönetim kurulu, organizasyonun risk iştahını belirleyerek üst yönetime yön verir. Yönetim kurulu, üst yönetimin risklere uygun şekilde tepki verilip verilemediğini sürekli olarak güvence altına alır. Yönetim kurulu, RY ve kontrol operasyonunun temel mülkiyet ve sorumluluğunu CEO’ya ve üst düzey yönetime delege eder. RY açısından çalışanlara liderlik ve yön verme ve organizasyonun genel kabul görmüş risk iştah seviyesi ile ilgili risk alma faaliyetlerini kontrol etme, yönetimin görevidir.[142]

[141] IIA Norge, **Guidelines For The Risk Management Function**, 2017.
[142] Chartered Institute of Internal Auditors, **Governance of Risk: Three Lines of Defence**, 2015, https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/



Şekil 12: Risk Yönetiminde Üç Savunma Hattı

Kaynak: Erdemir Grubu, http://tkib.gov.tr/wp-content/uploads/dosya-6024-3932.ppt

‘‘Üç Savunma Hattı Modeli’’ bir risk yönetim modeli benimsememiş işletmelerde dahi risk ve kontrollerin anlaşılmasına katkı sağlayabilir. ‘‘Üç Savunma Hattı Modeli’’, risk yönetiminde rol alan üç hatta ayrılır:[143]

• **Birinci Savunma Hattı** (Riski üstlenen ve yöneten birimler): Operasyonel Yönetim ve İç Kontrol Birimleri

• **İkinci Savuma Hattı** (Risklere nezaret eden birimler): Risk Yönetimi ve Uyum Birimleri

• **Üçüncü Savunma Hattı** (Bağımsız güvence sağlayan birimler): İç Denetim Birimleri

[143] IIA, **Etkili Risk Yönetimi ve Kontrolünde Üç Savunma Hattı,** Görüş Açıklamaları, 2013, TİDE (Çev.), https://www.tide.org.tr/uploads/PP_3_Savunma_Hatti.pdf

Birinci Savunma Hattı: Operasyonel riski elinde bulundurur ve yönetir, bu nedenle bu satırdaki çalışanlar tarafından gerçekleştirilen iç kontrolün yeterliliğini sağlamalıdır. Örn, satış elemanları, büro elemanları ve benzeri diğer işlevler. Hat yönetimi, etkin bir İK sürdürmekle yükümlüdür. Bu durum risk yönetimi ve risk tedavisinin mülkiyetini ve sorumluluğunu gerektirir. Günlük operasyonel kontrol faaliyetleri tipik olarak, operasyonel yönetim tarafından belirlenen limitler dahilinde bu hattaki personel tarafından gerçekleştirilir. Üst düzey yönetim, gerçekleştirilecek kontrollerin geliştirilmesine ve/veya izlenmesine katkıda bulunmak için çeşitli kontrollerin ve izleme işlevlerinin kurulmasından sorumludur. **İkinci Savunma Hattı**: Hem proaktif hem de reaktif olan bir role sahiptir. Proaktif tarafta, ikinci defans hattı, Örn: Risk yönetimi, yönetim ve karar verme ilkelerinin çerçevesinin geliştirilmesine ve performansa katkıda bulunulmasına ve birinci defans hattındaki faaliyetlerin geliştirilmesine katkıda bulunur. Reaktif tarafta, ikinci defans hattında raporları izleyecek ve örgütle diyalogu sürdürecektir. İkinci defans hattı destek ve kontrol faaliyetleri, Örn: Finans, uyum, RY, sağlık ve güvenlik, hukuk ve kalite yönetimi tarafından gerçekleştirilir. Spesifik fonksiyonlar organizasyon ve sektörlere göre değişiklik gösterecektir. **Üçüncü Savunma Hattı**: İD tarafından gerçekleştirilir ve iç denetimlerin tasarımı ve işletilmesi ile ilgili ikinci savunma hattından daha fazla bağımsız ve nesnel güvence veren yönetici organlar ve üst düzey yönetimler sağlar. İD, diğer şeylerin yanı sıra kurumun yönetişim ve kontrol süreçlerinin etkili olup olmadığını ve birinci ve ikinci savunma hatlarının etkin ve verimli çalışıp çalışmadığı da dahil olmak üzere iç kontrollerin işlev görüp görmediğini değerlendirir ve kuruluşun başarısına katkıda bulunur.[144]

[144] IIA Norge, **Guidelines For The Risk Management Function**, 2017, s. 15.

5.3. COSO Kurumsal Risk Yönetimi Modeli ve COSO İç Kontrol Modeli İlişkisi

İşletmelerde en çok tercih edilen ve 2013 yılında revize edilen ‘‘COSO İç Kontrol Bütünleşik Çerçevesi ve 2004 yılında yayınlanan ‘‘Kurumsal Risk Yönetimi Bütünleşik Çerçevesi’’ arasındaki bağlantıların analiz edilmesinin, İK ve RY kavramlarının arasındaki ilişkinin anlaşılmasını yardımcı olarak, İD alanında RY’nin kavramsal analizine önemli katkı sağlayacağı düşünülmüştür.

İç kontrolün gelişimi COSO komitesinin ERM modelini geliştirmesiyle bir başka boyuta, RY boyutuna taşınmıştır. Firmanın hedeflerini finansal raporlama konusundaki hedefleri de dahil olmak üzere gerçekleştirmesinin önündeki risklerin tanımlanması ve uygun kontrol yöntemleriyle giderilmesi, İK kavramını finansal raporların güvenirliğinin artırılmasının çok ötesinde, KRY’nin önemli bir unsuru haline getirmiştir. Bu gelişmeyi yansıtacak şekilde COSO komitesi, COSO İK modelini bir ileri aşamaya taşıyarak 2004 yılında ‘‘ERM Kurumsal Risk Yönetimi Bütünleşik Çerçevesi’’ni yayınlamıştır. Bu çerçeve ile İK kavramı, firmanın geleceğine ilişkin belirsizliklerin yönetilmesi hedefi doğrultusunda KRY önemli bir unsuru haline getirmiştir. İK kavramındaki bu gelişim KY kavramının gelişmesiyle çok yakından ilgisi vardır. KY kavramının gelişiminde sermaye sahibi olmanın verdiği hakların korunmasının büyük etkisi olduğu anlatılmıştır. Söz konusu gelişimde bir diğer önemli etken yanıltıcı finansal raporlamalardır.[145]

İK çerçevesi ile KRY çerçevesi arasındaki temel farklılıkların başında ise ilkinin İK esaslı, ikincisinin risk değerlendirme esaslı tasarlanmış olması gelmektedir. KRY kurumu etkileyebilecek risklerin anlaşılması ve yönetimi için tasarlanmışken, İK çerçevesi kurum içi faaliyetlerin bir gereksinimi olan iç kontrollerin anlaşılması ve yönetimi için tasarlanmıştır. İK çerçevesi RY’nin bir bileşeni olmakla birlikte burada ilgi

[145] Ç. Özbek, 2012, s. 399-400.

noktası, İK temelli risklerdir, öte yandan KRY işletme temelli risklerin yanı sıra organizasyon genelini ilgilendiren dış çevre kaynaklı riskleri de ilgi alanına eklemiştir.[146]

COSO İK modelinin risk değerlendirme bölümü ile KRY bölümünde incelenen hususlar büyük ölçüde örtüşmektedir. ERM modeli COSO İK modelinin risk değerlendirmesi başlıklı ikinci adımının daha da geliştirilmiş halini yansıtmaktadır. COSO modelinde sadece riskler dikkate alınırken, ERM risk yerine belirsizlik kavramını kullanmış ve belirsizliklerin risk doğurabileceği kadar fırsatlarda sunabileceğini ortaya koymuştur.[147]

Her ne kadar ERM kelimesi ile COSO komitesi tarafından geliştirilen ERM modeli aynı ismi taşısada, günümüzde KRY uygulamalarının birçoğunda yer alan prensipler, COSO ERM modelinin içeriğinden gelmektedir. ERM; tüm riskler için silo anlayışı ile değil, daha bütünsel bir yaklaşımla ele almakta, RY kapsamına tüm kurum faaliyetleri ve yönetsel süreçler dahil edilmekte, belirsizlikler sadece risk değil fırsat yaratma potansiyelinin de değerlendirilmesini içermektedir. RY süreç bazlı değil, stratejik bir yönetim modeli ortaya çıkmaktadır.[148]

ERM, portföy perspektifinden riske odaklanarak iç kontroller üzerine genişler. Örn: ‘‘İç Kontrol - Entegre Çerçeve’’; operasyon, finansal raporlama ve uygunluk gibi üç hedef kategorisini belirtir. ERM bu üç kategoriyi de içerir ve raporlama amacını genişletir. ‘‘İç Kontrol Bütünleşik Çerçeve’’ yayınlanan finansal tablolarla ilgiliyken, ERM, kurumun tamamında ortaya çıkan hem iç hem de dış raporlarla ilgilidir. Ayrıca ERM, kuruluşun misyonuna dayanan ek bir hedef kategorileri, yani stratejik hedefleri eklemektedir. ERM’de stratejik hedeflerin operasyonlara, raporlamaya ve uyumluluk hedeflerine uygun

[146] Moller Robert R., **Brink’s Modern Internal Auditing**, John Wiley & Sons, 2005’den aktaran D. Pehlivanlı, 2014, s. 70.
[147] Ç. Özbek, 2012, s. 424-425.
[148] Protiviti Inc., **Guide to ERM**, 2006, www.protiviti.com’dan aktaran Ç. Özbek, 2012, s. 262.

olması gerekir. ERM ayrıca, ‘‘İç Kontrol Entegre Çerçeve’’nin risk değerlendirme bileşenini dört bileşene bölerek, genişletir, bunlar; hedef belirleme, olay tanımlama, risk değerlendirmesi ve risk yanıtı bileşenleridir. COSO iç kontrol çerçevesi ve COSO ERM her ikisi de, risklerin bir şirketin her düzeyinde bulunduğu ve iç ve dış etkenlerden kaynaklandığını kabul eder. Bununla birlikte, ERM potansiyel olaylar konseptini tartışır. Olayların olumlu ve olumsuz etkileri olabileceğini kabul eder. ERM ayrıca riski en aza indirgemek ve potansiyel faydaları en üst düzeye çıkarmak için olayları tetikleyen şeyleri araştırır. Risk değerlendirmesi, ERM kapsamından daha ayrıntılı bir süreçtir. Son olarak, risk karşılığı seçenekleri ERM'de daha ayrıntılıdır. ERM, ‘‘COSO İç Kontrol Bütünleşik Çerçevesi’’nin diğer bileşenlerini de genişletir. ERM, bazı durumlarda kontrol faaliyetlerinin kendilerinin bir risk karşılığı olarak hizmet ettiğini vurgular. ERM geçmiş, şimdiki ve gelecekteki olaylardan elde edilen verilere odaklanarak bilgi ve iletişim bileşenini de genişletmektedir. Genel olarak ‘‘COSO, İç Kontrol Bütünleşik Çerçevesi’’, ‘‘ERM Risk Yönetimi Entegre Çerçevesi’’nin oluşturulmasında bir temel olarak kullanmıştır.[149]

COSO'nun 2004 yılındaki başkanı olan John Flaherty, ERM Integrated Framework'e ilişkin önsözünde: ‘‘COSO iç kontrol çerçevesinin politika kural ve düzenlemelere adapte edildiğini, kurum hedeflerinin gerçekleştirilmesi doğrultusunda faaliyetlerin daha iyi kontrol edilmesi amacıyla binlerce firma tarafından kullanıldığını, zaman içerisinde firmanın risklere yönelik kaygılarının artığını ve risklerin etkin bir şekilde tanımlanması değerlendirilmesi ve yönetilmesi için güçlü bir uygulama çerçeveye olan ihtiyacın çok açık hale geldiğini, ERM Integrated Framework'un KRY yönetimine daha geniş bir kapsamda ve güçlü bir şekilde odaklanarak iç kontrolü daha da genişlettiğini ancak aynı zamanda COSO İK modelinin yerini alması gibi bir amacının olmadığını, daha ziyade İK modeli ile birleştirmek amacını taşıdığını ve firmaların

[149] **COSO's Enterprise Risk Management - Integrated Framework**, https://erm.ncsu.edu/library/article/coso-erm-framework

KRY'ye, gerek İK ihtiyaçlarını gidermek için, gerekse daha detaylı bir risk yönetim uygulamasına doğru ilerlemeye karar verebileceklerini ifade etmektedir.''[150]

İK çerçevesine kıyasla ERM çerçevesi, RY üzerinde daha geniş bir odak noktası olup, İK çerçevesini içermektedir. ERM çerçevesi, yeni bir kategori olan stratejik hedefleri eklemiş ve raporlama hedefini iç raporlamaları içerecek şekilde genişletmiştir. ERM çerçevesinde risk iştahı ve risk toleransı kavramları ortaya çıkmıştır. ERM çerçevesi, risk değerlendirme bileşenini hedef belirleme, olay tanımlama, risk değerlendirmesi ve risk yanıtı olmak üzere dört bileşene genişletir. Roller ve sorumluluklar ise risk yönetimine yönelik iç kontrole odaklanmak üzere genişletilmiştir. ERM çerçevesinin iç çevre bileşenleri, risk yönetimine ağırlık vererek, İK çerçevesinin kontrol ortamı bileşeninin yedi özelliğini kapsar ve üç ek nitelik ekler, bunlar: RY felsefesi, risk kültürü ve risk iştahıdır.[151]

Yönetim, risk tolerans düzeylerini belirlerken, ilgili hedeflerin göreceli önemini göz önüne alır ve risk toleransını risk iştahıyla uyumlaştırır. Risk toleransı içinde çalışma, işletmenin, risk iştahının içinde kalmasının daha büyük bir güvence sağladığı ve bu da kuruluşun hedeflerine ulaşması için ek bir uygunluk sağladığı anlamına gelir. Risk toleransı kavramı, iç kontrole ön şart olmak üzere çerçeveye dahil edilir ancak iç kontrole dahil değildir. KRY, bir portföy perspektifinden gelen bileşik riskleri dikkate almayı gerektirir. Bu kavram, bireysel bazda hedeflere ulaşılmasına odaklanan ''İç Kontrol Bütünleşik Çerçeve''de düşünülmemiştir. İK, işletmenin bir portföy görünümü geliştirmesini gerektirmez.[152]

---

[150] COSO, **Enterprise Risk Management Framework**, Application Techniques, 2004, www.coso.org, s. 3'den aktaran Ç. Özbek, 2012, s. 262-263.

[151] Protiviti, **Guide To Enterprise Risk Management**, Frequently Asked Questions, 2006.

[152] COSO, **Internal Control - Integrated Framework**, Framework And Appendices, September 2012, Post Public Exposure Version, s. 173-178.

Hem ‘‘İç Kontrol Bütünleşik Çerçevesi’’ hem ‘‘Kurumsal Risk Yönetimi Bütünleşik Çerçevesi’’, işletmelerin içe ve dışa yayımlanan tüm raporlarını kapsar. Kurum risk yönetiminin altında yatan temel ilke, tüm paydaşlar için değer sağlamaktır. Stratejik hedefler, işletmenin paydaşları için değer yaratmaya nasıl başlayacağına ilişkin yönetimin seçimini yansıtır. KRY bir işletmenin değer yaratıp yaratmadığını, mevcut değeri konusuna odaklanırken, iç kontrolde ise daha önce belirtilen hedeflerin gerçekleştirilmesine odaklanır. KRY organizasyonun kabul etmeye istekli olduğu risk miktarını, risklerin hem stratejik seçimlerden nasıl yaratıldığını hem de hafiflettiğini ve ortaya çıkan risklerin kuruluşu nasıl etkilediğini göz önüne alarak, ileriye dönük olarak görülür. Buna karşılık İK, organizasyonun belirtilen hedeflerin başarılması için riskleri azalttığına odaklanmaktadır. İK genellikle daha geriye dönüktür, daha çok retrospektifdir.[153]

ERM, iç kontrolden daha geniştir ve doğrudan daha fazla riske odaklanmaktadır. İç kontrol ERM’nin ayrılmaz bir parçası iken, ERM genel yönetişim sürecinin bir parçasıdır. ERM çerçevesi, alternatif risk tepkileri ile ilgilenirken (riskten kaçınma, kabul, paylaşım ve azaltma), İK çerçevesi öncelikle risk azaltma ile ilgilidir. ERM, stratejik hedefler ve strateji belirleme üzerine odaklanır, zira stratejik hedeflere ulaşma dışsal olaylara bağlıdır. İç kontrol ise bunu sağlamaz.[154]

İK, KRY’nin içinde bulunur ve KRY’nin ayrılmaz bir parçasıdır. KRY, iç kontrole göre daha geniş kapsamlıdır. ‘‘COSO İç Kontrol Çerçevesi’’ hedef kategorilerinde, operasyonlar, finansal raporlama ve uyumluluk olmak üzere üç hedef kategorisini belirtir. KRY, operasyonlar, raporlama ve uyumluluk olmak üzere üç benzer hedef kategorisini belirtir. İK çerçevesindeki raporlama kategorisi, yayınlanmış finansal tabloların güvenilirliği ile ilişkili olarak tanımlanmaktadır. KRY çerçevesinde, raporlama kategorisi, bir

[153] COSO, **Internal Control - Integrated Framework**, Framework And Appendices, September 2012, Post Public Exposure Version, s. 173-178.
[154] Protiviti, **The Updated COSO Internal Control Framework**, Frequently Asked Questions, Third Edition, 2014, s. 27.

işletme tarafından geliştirilen ve hem iç hem de dışsal olarak yayımlanan tüm raporları kapsayacak şekilde önemli ölçüde genişletilmiştir. Bunlar, yönetim tarafından kurum içi olarak kullanılan ve diğer taraflara düzenleyici dosyalar ve raporlar da dahil olmak üzere dış taraflara verilen raporları içerir ve kapsam mali tablolardan yalnızca finansal bilgilerden değil, aynı zamanda mali olmayan bilgileri de kapsayacak şekilde genişletilmiştir. ‘‘Kurumsal Risk Yönetimi Entegre Çerçeve’’ başka bir hedef kategori kategorisi eklemiştir. (yani diğer hedef kategorilerinden daha yüksek bir seviyede faaliyet gösteren stratejik hedefler) Stratejik hedefler; bir kurumun misyonundan veya vizyonundan kaynaklanır ve işlemler, raporlama ve uygunluk hedefleri onlarla uyumlu olmalıdır. KRY, strateji belirleme sürecinde ve diğer üç kategorideki hedeflere ulaşılmasına yönelik olarak uygulanmaktadır.[155]

COSO ERM modelinin temelini, COSO komitesinin 1992 yılında yayınladığı ‘‘COSO İç Kontrol Bütünleşik Çerçeve’’ isimli İK modeli oluşturmaktadır. COSO İK çerçevesinin geliştirilme amacı finansal raporlama süreçlerindeki usulsüzlüklerin azaltılması ve bu süreçlerdeki iç kontrolün etkinliğinin artırılmasıdır. COSO çerçevesi her ne kadar kapsam olarak sadece finansal raporlama süreçlerini değil firmanın tüm operasyonlarını ve faaliyetlerindeki iç kontrollerin yeterlilik ve etkinliğinin değerlendirilmesinde önemi bir araç sunsada çıkış noktası finansal raporlamalar konusunda bir kontrol çerçevesi sağlamakta olup; COSO ERM modelinin firma hedeflerinin stratejik operasyonel raporlama ve mevzuata uyum olarak sınıflandırılmasının temelinde bu düşünce yatmaktadır. Ülkemiz uygulamaları açısında baktığımızda finansal raporlama elbette önemlidir ancak her sürecin birimin mutlaka çok yoğun bir raporlama yapması veya oldukça detaylı bir raporlama sistemine sahip olması gerekli olmamaktadır. Her bölüm veya birimin raporlama yükümlülüğü olmadığı gibi, her bölümün stratejik bir hedefi de olmayabilecek

[155] COSO, **Enterprise Risk Management - Integrated Framework**, Executive Summary, September 2004, http://ehss.moe.gov.ir/getattachment/2b57139a-e934-4f59-84f9-c9b46e385241/

bazı bölüm veya birimler sadece destek hizmeti sağlayan birimler olabilecektir. Bu durumda en ağırlıklı hedef sınıfının operasyonel hedefler olması çokta şaşırtıcı olmayacaktır.[156]

Hedefleri belirlenmemiş bir kurum için, İK sistemi tasarlamak ve uygulamak pratik değildir. Hedeflerin ve ilgili alt hedeflerin kurulması ve belirlenmesi, yasaların, kuralların, yönetmeliklerini, standartların ve yönetimin kendi tercihleri göz önünde bulundurması stratejik planlama sürecinin bir parçasıdır, İK, bir kurumun hedeflerinin ne olması gerektiğini kuruma dikte edemez veya hedeflerin belirlenmesine yönelik bir yapı kurmaz. ‘‘Kurumsal Risk Yönetimi Bütünleşik Çerçeve’’nin hedef belirleme bileşeni, yönetim ve yönetim kurulunun işlemleri, raporlamayı ve uygunluk hedeflerini belirlemek için kullandığı süreci değerlendirir. Risk iştahını ve risk toleransını ayarlamak, KRY'nin temel ilkeleridir. Buna karşılık İK, etkili bir İKS'ye ön koşul olarak hedeflerin ve risk toleransının durumunu göz önüne alır.[157]

5.4. Risk Yönetimi/Kurumsal Risk Yönetimi ve İç Denetim İlişkisi

UİDMUS'un terimler sözlüğünde, RY'yi, "kurumun amaçlarını gerçekleştirmek konusunda makul güvence sağlamak amacıyla potansiyel olay ve durumları belirleme, değerlendirme, yönetme ve kontrol etme süreci" olarak tanımlanmaktadır. Bu tanım, Uluslararası Standartlar Teşkilatı (ISO)'nun RY tanımına da uygundur: "Bir kurumu risk konusunda yönlendirmek ve kontrol etmek amacına yönelik eşgüdümlü faaliyetler." KRY kurum çapında RY olarak da kullanılmaktadır. COSO, bu terimi: "Kurumu etkileyebilecek potansiyel gelişmeleri ve olayları tespit etmek ve mevcut riskleri risk alma iştahı çerçevesinde yönetmek ve kurumun hedeflerine ve amaçlarına ulaşması konusunda makul

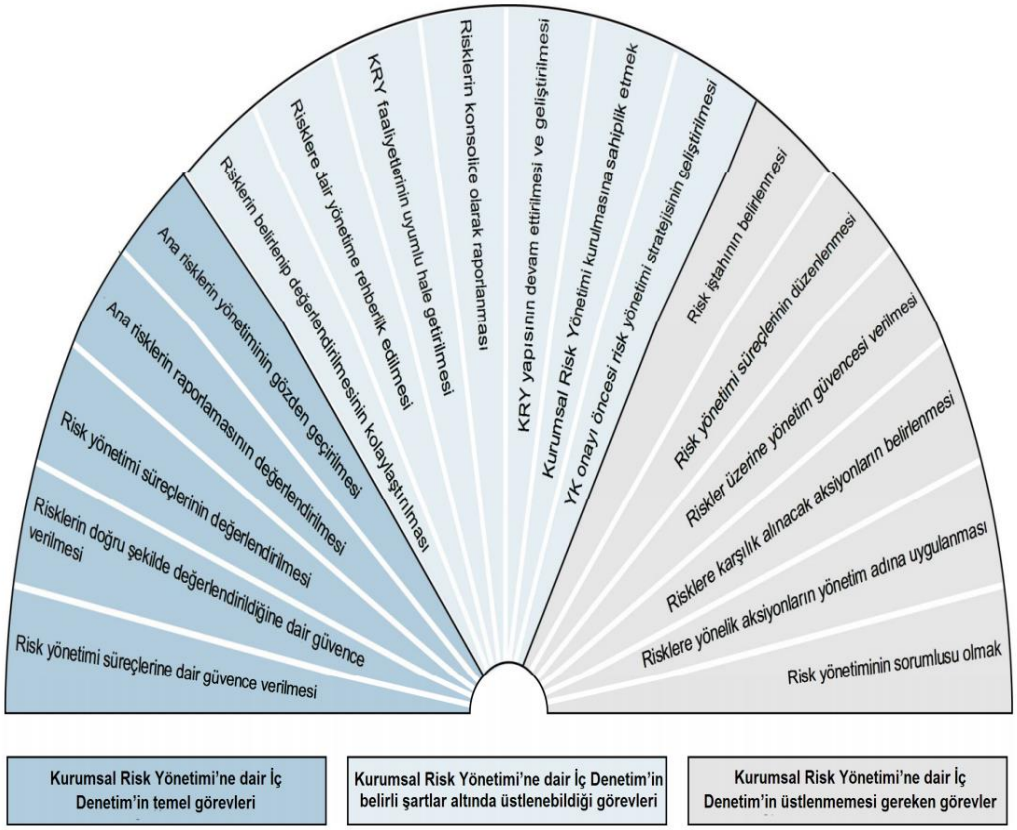
[156] Ç. Özbek, 2012, s. 314-315.

[157] COSO, **Internal Control - Integrated Framework**, Framework And Appendices, September 2012, Post Public Exposure Version, s. 173-178.

güvence sağlamak amacıyla tasarlanmış, kurum çapında ve strateji düzenlemesi alanında uygulanan ve kurumun yönetim kurulu, yönetimi ve başka personeli tarafından yürütülen bir süreç" olarak tanımlamaktadır.[158]

İD'nin KRY'ye ilişkin esas rolü ve görevi, risk yönetiminin etkinliği hakkında yönetim kuruluna objektif güvence vermektir. RY, kurumsal yönetimin temel unsurlarından biridir. İşletmede bir RY sistemi kurmak ve idame ettirmek yönetim sorumludur. İç denetçinin KRY konusundaki temel ve asli rolü, risk yönetiminin etkinliği hakkında hem yönetim kuruluna hem de kurum yönetimine güvence sağlamak olmalıdır. İDB faaliyetlerini bu temel ve asli rolünün ötesine geçirdiği ve genişlettiği takdirde, angajman ve görevlere danışmanlık hizmetleri muamelesini yapmak ve bu konuyla ilgili standartların tümünü uygulamak da dahil belirli koruma önlemleri almalıdır. Böylece İDB güvence hizmetlerinin objektifliğini ve kendisinin bağımsızlığını korumuş olacaktır. Bu kısıtlama ve sınırlamalar dahilinde KRY, İDB'nin profilinin yükseltilmesine ve etkinliğinin artırılmasına yardımcı olabilir.[159]

[158] IIA, **Risk Yönetimi ve Güvence Görevlerinin Koordinasyonu**, Uygulama Rehberi, Mart 2012, TİDE (Çev.), https://www.tide.org.tr/
[159] IIA, **İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol**, 2009.



Şekil 13: İç Denetimin Kurumsal Risk Yönetimindeki Rolü

Kaynak: IIA, **İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol**, 2009.

Şekil 13' de yelpazenin sol tarafında gösterilen faaliyetlerin tamamı güvence faaliyetleridir. Bunlar, RY hakkında güvence sağlamak olarak ifade edilir. Yelpazenin orta kısmında yer alan görevler, İD'nin belirli şartlar altında üstleneceği görevleri belirtmektedir. Sağ taraftaki gri alandaki görevler ise iç denetim faaliyetinin bağımsızlığına zarar vereceği gerekçesiyle üstlenilmemesi gereken görevlerdir.[160]

[160] IIA, 2009.

ALTINCI BÖLÜM

İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN GİRİFT İLİŞKİLERİNİ GÖSTEREN BİR MODEL ÖNERİSİ VE TARTIŞMALAR

İç denetim alanında RY kavramının mantıksal yerini belirlemek, bu amaçla iç denetimin tanımında yer alan ve iç denetimin kapsamını oluşturan (KY, İK, RY) kavramlarının aralarındaki etkileşimi ve ilişkiyi anlamak için, Şekil 14'de gösterilen bir genel çerçeve model önerisi hazırlanarak, bu model üzerinden altı adet öneri tartışmaya sunulmuştur. Şekil 14'de risk yönetiminin girift ilişkilerini gösteren bu model içindeki şekillere ve doğrusallara farklı numaralandırmalar yapılarak, öneriler bu numaraları referans göstererek hazırlanmıştır.

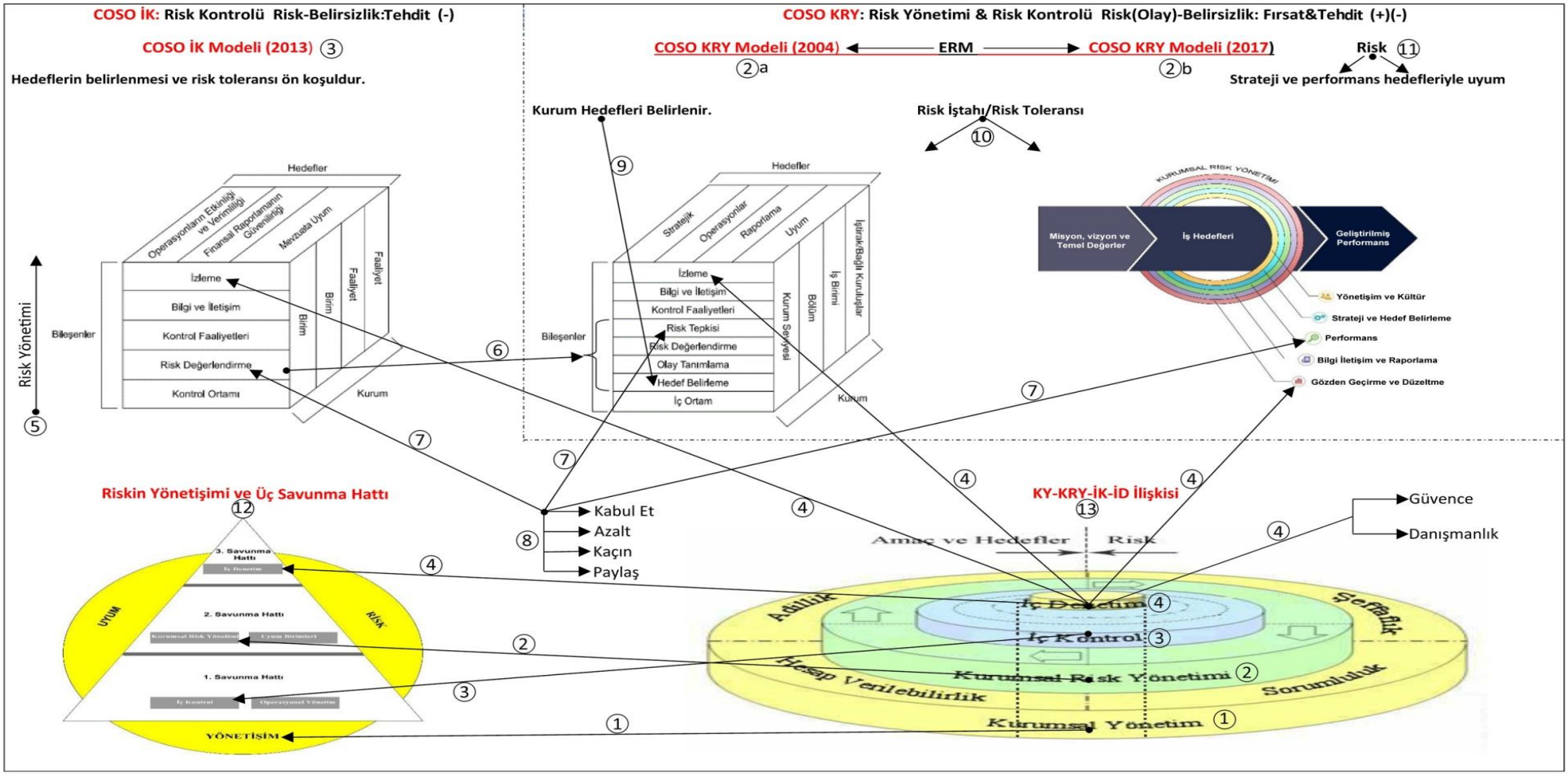
Bu modelde: Sağ alt kısımda yer alan ⑬ numaralı şekil olan: ''KY ①, KRY ②, İK ③, İD ④ ilişkisi'', katmanlara ayrılan üç boyutlu bir görsel üzerinde gösterilerek, kavramların birbirleri arasındaki kapsama alanına dikkat çekilmiştir. ⑬ numaralı şekille bağlantılı olarak, iç denetimin fonksiyonları ve iç denetimin COSO modelleri ile olan temasları, ④ numaralı doğrusallarla gösterilmiştir. Ayrıca ⑬ numaralı şekil ile ⑫ numaralı şekil olan ''Risk Yönetişimi ve Üç Savunma Hattı'' ilişkilendirilmiştir.

Çerçevenin üst kısmı, COSO İK ve COSO ERM modelleri için ayrılmıştır. COSO İK ve COSO ERM modelleri arasında; risk, hedef ve kontrol açısından farklı bakış açıları olduğunu kısaca belirtmek adına, bu modellerin bulunduğu başlıkların üst ve alt satırlarına kısa açıklamalar yapılmıştır. Çerçevenin sol üst kısmına, ③ numaralı şekilde gösterilen COSO İK Modeline ait COSO küpü yerleştirilmiş, COSO İK Modeli bileşenlerinin; RY, İD ve COSO KRY modeli ②a ile olan ilişkileri: ④, ⑤, ⑥, ⑦, ⑧ numaralı doğrusallar kullanılarak ilişkilendirilmiştir.

Risk yönetimini, KRY'den ayırmak, aynı zamanda risk yönetim sürecinin, COSO İK Modeli içinde var olduğunu göstermek için; ⑤ numaralı doğrusal, (risk yönetimi) adıyla, ③ numaralı şekil olan ve COSO İK modelini temsil eden küpün sağ tarafına yerleştirilmiştir.

Genel çerçeve modelin sağ üst tarafına: COSO komitesinin yayınladığı COSO ERM modellerinden olan, ②a numaralı şekilde gösterilen COSO 2004 KRY modeline ait COSO küpü ve ②b numaralı şekilde gösterilen, COSO ERM modelinin yakın zamanda güncellenen dökümanı ''COSO ERM Riskin Strateji ve Performansla Uyumlaştırılması Modeli'' yerleştirilmiştir. KRY temsil eden bu iki model, çerçevede üst kısımda, diğer şekillerden ayrı bir alanda gösterilmiştir. Bu modellerin kendine özgü detayları: ⑨, ⑩, ⑪, numaralı doğrusallarla, COSO İK modeli ve İD ile olan ilişkisi de; ④, ⑥, numaralı doğrusallarla gösterilmiştir.

Son olarak ⑫ numaralı şekilde: Riskin yönetişimi ve üç savunma hattı modeli gösterilerek, üç savunma hattında yer alan (KRY, İD, İK, KY)'nin konumları: ①, ②, ③, ④ numaralı doğrusallar kullanılarak, ⑬ numaralı görselle ilişkilendirilmiştir.



Şekil 14 : İç Denetim Alanında Risk Yönetiminin Girift İlişkileri Gösteren Bir Model Önerisi

Kaynak : Bu Model, COSO ve IIA' ya ait dökümanlardan alınan bilgi ve görseller yardımıyla oluşturulmuştur.

6.1. Öneri 1: Risk Yönetimi ve Kurumsal Risk Yönetimi Arasındaki Kavramsal Farklılıklar: ②, ⑤

Son yıllarda; kurum genelinde risklerin belirli bir stratejiyle kurumsal anlamda yönetilmesi anlayışının gerekliliğine olan ihtiyaç, KRY'nin işletmelerde giderek popülaritesini arttırması; RY yerine KRY kavramının, çeşitlik kaynaklarda sanki RY ile aynı anlamdaymış gibi kullanılmasına neden olmuştur. RY ve KRY birbirlerinden tamamen farklı kavramlar olup; KRY, risk yönetiminin günümüzde en yaygın olarak kullanılan, stratejik RY modelinin en son ve en yeni uygulama şeklidir.

RY, KRY'yi de içine alan genel bir kavramdır, aynı zamanda RY'de KRY'nin bir parçasıdır. İki kavram iç içe geçmiştir. Bir kurumda RY uygulanıyor denildiğinde, uygulanan RY şeklinin kurumsal risk yönetimi mi geleneksel risk yönetimi mi olduğuna dair bir yorum yapamayız. RY kavramı genel bir RY anlayışını yansıtır. Her kurum farkında veya farkında olmadan formel/informel bir RY faaliyeti uygular. İşletmeler, hedeflerine varmayı engelleyecek olumsuz durumların yarattığı riskleri bertaraf etme refleksini sergilemek zorundadırlar. KRY ise; belirli modeller aracılığıyla uygulanan formel bir anlayıştır, bilinçli olarak kuruma entegre edilmiştir ve işletmenin isteğine bağlıdır. Bir işletmede KRY'nin varlığından söz ediliyorsa, o işletmede RY uygulanıyor diyebiliriz ancak bir işletmede RY mevcuttur dediğimizde, o işletmede KRY'nin uygulandığını garanti edemeyebiliriz.

Bu bağlamda iç denetimin IIA tarafından yapılan güncel tanımına baktığımızda KRY değil, RY kavramını kullanıldığını ayrıca belirtmek gerekir. IIA tarafından yapılan iç denetimin tanımında genel bir ifade olan RY kullanılıyor olması doğru bir yaklaşımdır. Çünkü bazı kurumlar çeşitli coğrafi, yapısal, kültürel ve yasal farklılıklardan nedeniyle KRY uygulama imkânı bulamayabilirler. Global İD tanımının kapsayıcı olması gerekir. RY, KRY'ye göre daha genel bir kavramı yansıtır. Öte yandan, IIA yayınladığı uygulama

önerileri, rehberleri ve pozisyon raporlarında sıklıkla RY yerine KRY kavramını kullanmaktadır.

IIA, ‘‘İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol’’ isimli pozisyon raporunda bir kurumun yönetişim süreçlerini en iyi KRY yoluyla geliştirme olasılığı ve imkânı bulunduğundan dolayı, özellikle kurumsal risk yönetimiyle ilgilendiğini beyan etmiştir.’’[161] Bu yaklaşımdan çıkarılacak sonuç, IIA'nın yönetişim süreçlerine katkı sağlayacağını düşündüğü için, KRY ile ilgilendiğini beyan etmesidir.

6.2. Öneri 2: Üç Savunma Hattı, İç Denetim, Kurumsal Yönetim, Kurumsal Risk Yönetimi, İç Kontrol, Hedef ve Risk Kavramları Arasındaki İlişkiler: ①, ②, ②a, ②b, ③, ④, ⑫, ⑬

Bir kurumda KRY ve İK çerçevesi olarak COSO İK ve/veya COSO ERM modelleri tercih edilmişse, iç denetim faaliyeti kurumca benimsenen bu modellerin izleme bileşenlerinde aktif rol oynayarak, İK ve KRY süreçlerinin etkinliğini ve verimliliğini değerlendirmeye ve geliştirmeye yönelik bağımsız değerlendirmelerle destek olur. İDF, vermiş olduğu güvence ve danışmanlık hizmetleriyle süreçlerin gelişimine katkı sağlar. Bu anlamda Şekil ⑬'de gösterilen katmanlı tabakalarda İD; KY, KRY, İK'nın tam merkezinde yer alır ve hepsine temas eder. KRY sürecine veya İK sürecine yönelik güvence/danışmanlık sağlayan bir İDF, aynı zamanda KY süreçlerine de kendiliğinden hizmet etmiş olacaktır. Burada dikkat edilmesi gereken ayrıntı, tüm bu süreçlerdeki denetimin risk odaklı yapılacak olmasıdır. ⑬ numaralı şekilde katmanı oluşturan her tabaka: ①, ②, ③, ④ risk ile yakından ilgilidir. Hedeflerin olmadığı bir ortamda riskten bahsedilemeyeceği de düşünüldüğünde, amaç/hedefler ve risk şekil

[161] IIA, **İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol**, 2009.

⑬'de dikey düzlemin sağ ve sol kısmında belirtildiği üzere, bu katman tabakaların tam ekseninde yer alır ve ilişkilidir.

Şekil ⑬'deki katmanlı tabakalar; hangi kavramın, hangi kavramın parçası olduğunun belirtilmesi, iç denetimin bu katmanlar içindeki konumunun anlaşılması açısından önemli bir görseldir. Bu görselde: İD, KY, KRY, İK birbirlerini kapsayan katmanlara ayrılmıştır. İD de bir katman olarak şekilde gösterilmiştir ancak İD'nin konumu diğerlerinden farklı olarak: KY, KRY, İK'nın hepsini birden kapsayarak, aynı zamanda bu kavramların merkezinde bulunmasıdır.

Riskin yönetimi, kontrolü, uyum fonksiyonları ve iç denetim birimlerinin arasındaki konumun belirlenmesi ve karşılıklı eşgüdüm içinde çalışılması, iyi bir risk yönetişimi ile mümkündür. IIA tarafından önerilen üç savunma hattı, riskin yönetişimini güçlendirmek adına uygulanması gereken faydalı bir modeldir. ⑫

Üç savunma hattı modelinde, iç kontrol daha çok bölüm seviyesinde operasyonel hedef ve risklerle ilgilenen bir sistem olduğu için, birinci savunma hattına yerleştirilmiştir. Çünkü portföy bakış açısıyla KRY faaliyetleriyle belirlenen kurumsal bir risk, operasyonel seviyedeki riski yansıtmayabilir. (Birim yöneticileri ile üst düzey yöneticiler arasındaki iletişim çoğu zaman sağlıklı olmayabilir.) Operasyonel seviyedeki bir faaliyete yönelik; hedefleri, riskleri ve kontrolleri en iyi alt kademedeki yöneticiler bilir. Bu yüzden iç kontrol birinci savunma hattında yer alır ve hedefler; liderlik seviyelerinde, birim çapında belirlenir.

İç kontrol, kurumların ilk defans hattını oluşturur. Ancak bu durumun olumsuz yanları da olabilir. Örneğin bir pazarlama departmanı yöneticisi, kendi departmanına ait süreçlerde, yasal bir risk, belirleyebilir. Ancak bu yasal risk, kurum genelinde bir itibar riskine de yol açabilir. Bu yüzden bütünsel risk yaklaşımı, ERM (KRY)'de daha önemli hale gelir. ERM, üç savunma hattında, uyum birimleriyle birlikte, ikinci hatta yer alarak

birinci savunma hattına destek olur. Üçüncü savunma hattında yer alan iç denetim faaliyeti de, bir ve ikinci savunma hattına yönelik bağımsız değerlendirmelerle, kurum faaliyetlerine destek olur.

Son olarak Şekil ⑬'de, katmanlı tabakalardaki kavramların birbirleriyle olan konumsal ilişkileri, Şekil ⑫'de bulunan üç savunma hattı modeli ile örtüşmektedir.

Şekil ⑫'de; birinci savunma hattına, İK ve operasyonel yönetim yerleştirilmiştir. RY/KRY ise, uyum birimleriyle ikinci savunma hattındadır.

Şekil ⑬'de; KRY, KY'nin parçası iken; İK, KRY'nin parçasıdır. Şekil ⑫'de üçüncü savunma hattında yer alan İD de, bütün bu kavramların parçası, aynı zamanda destekçisi ve değerlendiricisi olarak diğerlerinden daha özel bir konuma sahiptir.

6.3. Öneri 3: Kurumsal Risk Yönetimi/Risk Yönetimi ve İç Kontrol Kavramları Arasındaki İlişkiler: ②, ②a, ③, ⑤, ⑥

Risk yönetiminin en girift ilişkisi, iç kontrolle olan ilişkisidir. İki kavram sıklıkla karıştırılır ve uygulayıcılar bu iki kavramı zihinlerinde mantık zeminine oturtmakta zorlanır. Bu durumun sebebi; riskin kontrolü ve risk yönetimi kavramlarının birbirleriyle aynı anlamda algılanması, COSO modelleri kapsamında yayınlanan küplerinin benzer bir yapıda oluşu, yayınlanan çerçevelerin birbirilerinin yerini aldığına veya yeni yayınlanan bir modelin eskisini pasifize ettiğine olan yanılgılar başlıca nedenler olarak sayılabilir. (Yenilenen COSO ERM'de küp şeklinde olan gösterim kaldırılmıştır)

İç kontrol kendi içinde bir risk kontrolü ile risk yönetimini kapsamaktadır. Kafa karıştırıcı durum burada başlamaktadır. İK, riskleri azaltmaya/hafifletmeye yönelik uygulanan bir risk yönetim stratejisidir. Doğal olarak bir risk yönetim şeklidir. İK unsurları yada COSO İK modeli bileşenleri (kontrol ortamı) ile başlar. Sırasıyla; risklerin analiz

edilip değerlendirildiği, risk aksiyonlarının hazırlandığı (risk değerlendirme) ve bu aksiyonlara yönelik politika ve prosedürlerin belirlendiği kontrol faaliyetleri, bilgi/iletişim ve izleme bileşenleri ile devam eder. Bu süreç tam anlamıyla bir risk yönetim sürecidir. Sonuç olarak KRY, İK'yı kapsar, İK de içinde RY süreci barındırır diyebiliriz. Ancak İK kurumlarda, RY'den tamamen farklı bir konum ve uygulama içeriğine sahiptir.

Kurumlar İK ve KRY uygulamaları için bazı standartlar ve çerçeveler benimserler, bu çerçevelerden en kabul görmüş olanları, COSO komitesinin yayınladığı; COSO İK ve COSO ERM modelleridir. COSO ERM 2004 küpünün dört bileşeninin (hedef belirleme, olay tanımlama, risk değerlendirme, risk tepkisi) ⑥, COSO İK modelinin risk değerlendirmesi bileşeninin genişletilmesiyle oluşturulduğu dikkate alındığında, COSO İK ③ ve COSO ERM 2004 ②a modellerinin, birbirlerinin güçlü tamamlayıcısı olduğu söylenebilir. Yani iki modeli birbirinden bağımsız düşünmek mümkün değildir.

İK veya COSO İK modeli, riskin yaratacağı belirsizliği tehdit olarak, yani negatif görür. (-)

KRY veya COSO ERM modeli ise, riski olay diye adlandırır ve olayların yaratacağı belirsizliklerin fırsatları ve tehditleri oluşturabileceğini söyler. Bu yüzden riski hem negatif, hem de pozitif algılar. (-)(+)

İK/COSO İK risklerin kontrolüne odaklanırken, KRY/COSO KRY ise hem risklerin kontrolüne hem de yönetimine odaklanır. Bu durum, yani risk yönetiminin (risk kontrolünü de içine alan geniş bir kavram olduğu düşünüldüğünde) COSO ERM'nin COSO İK'yı kapsadığını gösterir. COSO KRY Modeli, COSO İK modelinin geliştirilmesi ve genişletilmesinden oluşmuştur.

6.4. Öneri 4: Risk Yönetimi ve *Risklerin Yönetimi* Arasındaki Kavramsal Farklılıklar: ②, ⑤, ⑦, ⑧

Risk yönetimi ile *riskin (risklerin)* yönetilmesi kavramları arasında da bir kavram karmaşası vardır. Risklere karşı alınacak aksiyonların uygulandığı, riskleri gidermenin (tedavi etmenin) yani risklere cevap verme seçeneklerinin değerlendirildiği süreç, *riskin yönetilmesi* şeklinde ifade edilir. Riskten kaçınmak, paylaşmak, kabul etmek veya azaltmak birer riske cevap verme (risk response) olup, kavramsal anlamda *riskin yönetilmesi* (risk yönetim stratejileri) şeklinde ifade edilir.

Risk yönetimi ise, genel anlamda risklerin belirlenmesinden başlayan ve gözetim kontrol ve raporlamaya kadar uzanabilen içine risklerin giderilmesini de alan genel bir süreci kapsar. ②, ⑤

Risklerin yönetimi veya *riskin yönetimi*, bir karar alma sürecidir ve çeşitli alternatiflerin değerlendirildiği, risklerin tedavi edilmesi için gerekli eylemleri açıklar. Risklere cevap verilecek aksiyon türlerini ifade eder. ⑧ Riskler, analiz edilip değerlendirildikten sonra gerekli kontrol faaliyetleri/aksiyonlar ile giderilir. Bu durum, *risklerin yönetilmesi* kavramını ortaya çıkarır. *Risklerin yönetimi*, risk yönetimi ile aynı anlamda değildir. *Risklerin yönetimi*, risk yönetim sürecinin bir parçasıdır.

6.5. Öneri 5: COSO İç Kontrol ve COSO ERM 2004 Modellerinde, Risk Değerlendirme ve Kontrol Faaliyetleri Bileşenleri Arasındaki İlişkiler: ②a, ②b, ③, ⑥, ⑦, ⑧

Bu kavramlar arasında, algıda farklılık yaratan durumlar vardır. İK, riskleri azaltmaya yönelik politika prosedür iken, İKS sistemi (örneğin: COSO İK) bir bütün halde olan yönetsel bir araçtır ve genel bir yapıyı temsil eder. İç kontroller; İKS'nin parçasıdır ancak kavramsal olarak birbirinden farklıdır.

İç kontrol kavramı; tekil anlamda bir iç kontrol sistemini (bir İKS yapısını örn: COSO İK modelini), çoğul anlamda (iç kontrolleri, yani bir İKS'den farklı olarak kontroller bütününü) ifade etmektedir.

COSO İK bileşenlerinden ''kontrol faaliyetleri'', riskleri azaltmaya yönelik politika prosedürleri eyleme geçirecek faaliyetler olarak bilinir. COSO ERM 2004 bileşenindeki ''kontrol faaliyetleri'' de risklere verilecek cevapları uygulamaya yönelik politika prosedürleri eyleme dönüştürecek faaliyetlerdir. COSO ERM 2004'de, COSO İK modelindeki gibi ''kontrol faaliyetleri'' adıyla bir bileşen kullanması, COSO 2004 ERM için uygundur ancak tam anlamıyla ERM'yi yansıtmamaktadır. Çünkü COSO ERM'de kontrol etmek kavramından çok, yönetmek kavramının işlenmesi gerekmektedir. 2017 yılında yenilenen COSO ERM'de ''kontrol faaliyetleri bileşeni'', içerik ve uygulama anlamıyla devam ederken, ''kontrol faaliyetleri'' adıyla bir bileşenin tanımlanmamış olması ise dikkat çekicidir.

COSO İK modelinde, risk değerlendirme bileşeninde, analiz edilip değerlendirilen risklere yönelik cevap verme yöntemleri (kabul et, kaçın, paylaş, azalt) ⑧ hakkında ayrıntılı bilgi verilmemiş, özellikle İKS'yi etkiyecek durumlara odaklanılması gerektiği belirtilmiştir. Nihayetinde COSO İK modeli ③ risklerin kontrolü ile ilgilidir. Riskleri

azaltmak/hafifletmekte iç kontroller ile mümkündür. COSO İK kontrol faaliyetleri bileşeni, riskleri azaltmak için politika ve prosedürlerle belirlenen eylemleri ifade ederek, İKS'nin risklere vereceği tepkiyi, riskleri azaltan iç kontroller olarak belirterek, alan daraltılmıştır. Fayda maliyet açısından etkin bir kontrol varsa ve bu kontrol riski azaltıyorsa, riske cevap olarak (azalt) seçeneği tercih edilmiş olacaktır. Bu mümkün değilse (kabul et, kaçın ya da paylaş) seçenekleri değerlendirilebilir. Riske cevap yöntemlerinden (azalt) seçeneği, iç kontrollere her zaman daha yakındır. Çünkü iç kontroller, riski (azaltma) ile ilgilidir. Kısmen riskin (paylaşılması da) riskin şiddetini azalttığı için (azalt) seçeneği ile birlikte COSO İK'nın riske cevap seçeneği olarak düşünülebilir.

COSO ERM 2004 modelinde ②a ise, riske cevap yöntemleri detaylı olarak ayrı bir bileşen altında (risk tepkisi) ⑥ açıklanmıştır. Kabul et, azalt, paylaş, kaçın, gibi seçenekler, ERM mantığıyla (risklerin yönetimi ile) doğrudan uyuşmaktadır. Risk tepkisi bileşenine bağlantılı olarak, COSO ERM 2004'de, kontrol faaliyetleri bileşeni; ''yanıtlarının gerçekleştirilmesine yönelik'' eylemleri belirleyen politika ve prosedürler olarak tanımlanmıştır. Kontrol faaliyetleri bileşeni, COSO İK modelindeki kontrol faaliyetleri bileşenindeki gibi ''azaltan'' ifadesi ile sınırlandırılmamıştır. COSO ERM 2004 bu açıdan değerlendirildiğinde, hem riski kontrol eden (azalt seçeneğini devreye alabilen yani iç kontrolleri kapsayan) hem de yöneten (kabul et, azalt, paylaş, kaçın ve gerektiğinde fırsatları da düşün) bir model olarak karşımıza çıkmaktadır.

6.6. Öneri 6: COSO İç Kontrol ve COSO ERM 2004 Modellerinde Hedef Kavramları Arasındaki Farklılıklar: ②a, ②b, ③, ⑨, ⑩, ⑪

A) COSO İç Kontrol Modelinde Hedefler: ③

Organizasyonun ana ve alt hedeflerinin tanımlanması, yönetimin stratejik planlama sürecine aittir. (misyon/vizyon, risk iştahı/toleransı gibi etkenler bu noktada devreye girer) Hedefler, kurum stratejileri ve risk iştahıyla uyumlaştırılır. Stratejik planlama süreciyle belirlenen hedef belirleme adımının, risk yönetiminin bir parçası olduğu düşünüldüğünde, bir kurumun KRY tesisini kurmadan İK yapısı kurması uygun değildir. Çünkü genel (ana) ve alt hedeflerini belirlememiş bir kurumun, iç kontrol sistemini devreye alması; iç kontrolün risklere, risklerin ise hedeflere göre belirlendiği düşünüldüğünde doğru bir yaklaşım olmayacaktır. COSO İK modelinde, COSO ERM'de ki gibi ayrı bir hedef belirleme bileşeni bulunmamaktadır.

Peki, bu durumda COSO İK küpünün üst yatay kısmında belirtilen (faaliyet/uyum/raporlama) hedefleri ne anlama gelmektedir. Bu hedefler, çoğunlukla birim/departman bazında ulaşılmak istenen spesifik kurum hedeflerinden oluşmaktadır. Bu hedeflerin, kurumun genel (ana) hedefleri ile uyumlu hale getirilmesi gerekir. Özetle, kurumun genel hedefleri ve risk toleransının, iç kontrol sistemi kurulmadan belirlenmiş olduğu varsayılır. Alt birimler, kendi faaliyetlerine özgü, kurumun ana hedefleri ve risk toleransına uygun hedefler (operasyonel, raporlama, uyum) belirleyebilir.

B) COSO 2004 ERM Modelinde Hedefler: ②a, ⑨, ⑩

COSO ERM 2004, COSO iç kontrol modelindeki hedef kategorilerine (faaliyet/uyum/raporlama) stratejik hedefleri de ekleyerek, bu hedeflere engel teşkil edebilecek veya fırsata çevrilebilecek olayları gündemine almıştır. Ayrıca ERM'de, hedef belirleme bileşeni (kurumun genel hedeflerinin belirlenmesi) olarak ayrıca bir bileşen tanımlanmış-

tır. ERM, bir risk yönetim modelidir ve İK'dan farklı olarak hedef belirleme adımı, modele baştan bileşen olarak entegre edilmiştir. Kurumun ana ve genel hedefleri, stratejiyi de dikkate alarak, ERM içinde belirlenir ve diğer raporlama/faaliyet/uyum hedefleri için temel oluşturur. Bu noktada, risk iştahı, risk toleransı, misyon/vizyon gibi kavramlar ERM'de detaylı şekilde tanıtılmış ve belirgin hale getirilmiştir.

C) COSO ERM 2017 Modelinde Hedefler: ②b, ⑩, ⑪

Yenilenen COSO ERM'nin adı ''Riskin Strateji ve Performansla Uyumlaştırılması Modeli'' olarak belirlenmiştir. COSO ERM 2004, stratejik hedeflere yoğunlaşmakta ve stratejik riskleri belirlemeye odaklanmaktadır. Yenilenen COSO ERM ise, stratejiye ait risklerin tek boyutta olmadığını açıklamıştır. Her stratejinin temel değerleri, performans kriterleri vd. özelliklerinin farklı olması, stratejilerin kendi içinde farklı etkilerini yaratacak, buda farklı risk profillerine sahip olmasına neden olacaktır. Yenilenen model, ERM'yi tüm stratejilerle uyumlaştırmayı sağlama amacındadır. Risk iştahı ve toleransı yeniden düzenlenmiştir. Yenilenen modelin diğer bir özelliği; riski, performans (risk değerlendirme) bileşeniyle de uyumlaştırmasıdır. Strateji ve iş hedeflerine ulaşmayı engelleyecek riskler, performans bileşeni altında belirlenir ve değerlendirilir. Önceki modellerden farklı olarak yenilenen ERM'de risk değerlendirme bileşeni yerine, performans bileşeni kullanılması, ERM'nin strateji ve performans hedeflerini engelleyebilecek risklere yoğunlaşması, risk değerlendirmesini diğer çerçevelerden farklı bir boyutta ele alması anlamına gelmektedir.

SONUÇ

İç denetim alanında risk yönetimi, önemli ve tartışılması gereken bir konuma sahiptir. Risk yönetiminin, iç denetim kapsamının en önemli unsurlarından olan iç kontrol ve kurumsal yönetim ile olan etkileşimi göz önüne alındığında, çeşitli kavramsal tartışmaların ortaya çıkması son derece doğaldır.

Bu tartışmaların temelinde; uluslararası alandaki kavramlara yüklenen ve sürekli güncellenen anlamlar, uluslararası kavram terminolojisi ile bu kavramların ülkemizdeki algılanışı arasındaki farklılıklar, COSO örgütü tarafından yayınlanan çerçeveler arasındaki benzerlikler ve ayrışmalar yatmaktadır.

COSO örgütü tarafından işletmelerde uygulamaların formel bir anlayışta etkin yürütülebilmesini sağlamak amacıyla çeşitli raporlar yayınlanmıştır. Bilindiği üzere COSO, 1992 yılında ilk raporu olan iç kontrol bütünleşik çerçeve raporunu yayınlamış, iç kontrol ile ilgili olan bu rapor, 2013 yılında revize edilmiştir. Değişen sektörel koşullar ve zaman içinde risk kavramının farklı boyutlara evrimleşmesi nedenleriyle, COSO örgütü iç kontrol raporu haricinde 2004 yılında COSO ERM adlı dökümanı da yayınlayarak, kurumsal risk yönetimi uygulamalarına yol gösterici bir model oluşturmuştur. Son olarak 2017 yılında COSO ERM raporu da yeni bir isim altında yenilenmiştir.

COSO tarafından iç kontrol ve risk yönetimi hakkında yayınlanan bu çerçeveler birbirlerinin tamamlayıcı unsurları olmakla birlikte, farklı perspektiflere sahiptir.

Bu çalışmada son bölümde, IIA'nın bakış açısı da dikkate alınarak, iç denetim alanında risk yönetimini ilgilendiren tüm COSO çerçeveleri tek bir öneri model üzerinde toplanmış ve çerçeveler görsel boyutta konumlandırılarak birbirleriyle ilişkilendirilmiştir. Bu ilişkilendirmelerle, işletmelerde çalışanlar arasında; risk yönetimi, kurumsal risk yönetimi, iç kontrol, iç denetim, kurumsal yönetim konularında ortak bir algının oluşmasına katkı sağlamak amacıyla, toplamda altı öneri sunulmuş ve sunulan bu öneriler ayrı başlıklar altında tartışılmıştır.

Girift ilişkileri gösteren bu öneri model üzerinden yapılan kavramsal çıkarım ve öneriler; çoğunlukla teorik mahiyette olup, kurumların kendilerine özgü pratik uygulamalarında farklı anlayışlar ve değerlendirmeler ortaya çıkabilmektedir.

İşletmelerde risk yönetimi, iç kontrol ve iç denetim faaliyetlerinde rol alan çalışanların; bu çıkarım ve önerileri dikkate alması, zihinlerinde kavramsal anlamda risk yönetiminin içselleştirilmesine katkı sağlayarak, RY uygulamalarında etkinliği ve verimliliği artıracaktır. Benzer şekilde bu çalışmada önerilen model, ileride bu alanda yapılması muhtemel akademik çalışmalarda bir rehber görevi görebilir ve geliştirilmeye açıktır.

KAYNAKÇA

Arslan, Işılda, (2008), **Kurumsal Risk Yönetimi**, Maliye Uzmanlığı Tezi, Türkiye Cumhuriyeti Maliye Bakanlığı, Strateji Geliştirme Başkanlığı, Ankara, s. 19-20.

Burca, Nazif, (2017), **Yenilenen COSO Kurumsal Risk Yönetimi Çerçevesi**, https://nazifburca.com/2017/09/20/yenilenen-coso-kurumsal-risk-yonetimi-cercevesi/, (01.11.2017).

Chartered Institute of Internal Auditors, (2015), **Governance of Risk: Three Lines of Defence**, https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/, (22.11.2017).

Chartered Institute of Internal Auditors, (2017), **Risk Appetite And Internal Audit**, https://www.iia.org.uk/resources/risk-management/risk-appetite/, (01.12.2017).

Chesley, D., Pett, J., Martens, F., **Powerful Complements: The Value of ERM And Internal Control Together**, http://www.pwc.com/gx/en/services/advisory/consulting/risk/resilience/publications/value-of-erm-and-internal-control-together.html, (05.11.2017).

Chesley, Dennis, (2017), pwc, **The Top Changes to The COSO ERM Framework You Need To Know Now**, http://pwc.blogs.com/resilience/2017/09/the-top-changes-to-the-coso-erm-framework-you-need-to-know-now.html, (06.01.2017).

COSO's Enterprise Risk Management - Integrated Framework, https://erm.ncsu.edu/library/article/coso-erm-framework, (15.10.2017).

COSO, (1992), **Internal Control Integrated Framework**, s. 14-133. www.coso.org/

COSO, (2004), **Enterprise Risk Management Integrated Framework**, www.coso.org/

COSO, (2004), **Enterprise Risk Management Framework**, Application Techniques, www.coso.org/, s. 3-53.

COSO, (2004), **Enterprise Risk Management - Integrated Framework**, Executive Summary, http://ehss.moe.gov.ir/getattachment/2b57139a-e934-4f59-84f9-c9b46e385241/, s. 61-83, (15.06.2017).

COSO, (Aralık 2011), **Internal Control Integrated Framework Exposure Draft**, www.coso.org/

COSO, (2012), **Internal Control - Integrated Framework**, Framework And Appendices, Risk Assesment, http://aechile.cl/wp-content/uploads/2012/11/coso_framework_body1.pdf, s. 13, (12.11.2017).

COSO, (Eylül 2012), **Internal Control - Integrated Framework**, Framework And Appendices, Post Public Exposure Version,http://aechile.cl/wp-content/uploads/2012/11/coso_framework_body1.pdf, s. 173-178, (18.07.2017).

COSO, **COSO 2013 İç Kontrol Çerçevesi**, https://denetimsitesi.wordpress.com/2014/08/15/coso-2013-ic-kontrol-cercevesi-3/, (02.09.2017).

COSO, (2017), **Enterprise Risk Management Integrating with Strategy And Performance**, Executive Summary, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf, (02.12.2017).

COSO, (June 2017), **Enterprise Risk Management Integrating with Strategy and Performance**, Frequently Asked Questions, https://www.coso.org/Documents/COSO-ERM-FAQ-September-2017.pdf, (05.12.2017).

Erdemir Grubu, http://tkib.gov.tr/wp-content/uploads/dosya-6024-3932.pptx, (16.10.2017).

Fıkırkoca, Meryem, (2003), **Bütünsel Risk Yönetimi**, Ankara: KalDer Yayınları, s. 14-15.

Galloway, David, (1995), **Internal Auditing: A Guide For The New Auditor**, Uluslarası İç Denetçiler Enstitüsü, USA.

Gleim Publications, Inc, (2015), **Control Framework and Fraud**, Study Unit Four, Türkiye İç Denetim Enstitüsü (Çev.), s. 4-11, https://www.gleim.com/, (28.10.2017).

Griffiths, David, **Risk Based Internal Auditing**, Version 2. 2, http://www.internalaudit.biz/, s. 5, (30.11.2017).

Günererdem, Deniz Ezgi, (2006), **Kamu İç Denetimde Kalitenin Sağlanması: İç Denetimde Kalite Güvence Sistemleri**, Türkiye Cumhuriyeti Maliye Bakanlığı, Devlet Bütçe Uzmanlığı Araştırma Raporu, Ankara, https://www.bumko.gov.tr/Eklenti/5487,denizezgiakinpdf.pdf?0, s. 17, (17.09.2017).

IIA, **Definition of Internal Auditing**, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx, (03.11.2017).

Internal Control System http://www.objectivecontrols.com/internal_control_system.html, (03.03.2017).

ISO, **ISO 31000 Risk Management Principles And Guidelines**, First Edition 2009-11-15, http://ehss.moe.gov.ir/getattachment/56171e8f-2942-4cc6-8957-359f14963d7b/ISO-31000, s. 18, (15.10.2017).

Kahyaoğlu, Sezer Bozkuş, **Kurumsal Risk Yönetimi Standartları**, Grant Thornton, http://www.gtturkey.com/ud_objs/pdf/etknlk/musiad_risk_yonetimi_sunumu.pdf, s. 6, (10.06.2017).

Kalyoncu, Demet, (2013), **Risksiz Risk Yönetiminin Alternatif Yolları**, Yüksek Lisans Tezi, Okan Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Kaya, Bertan, (2014), **İç Denetime İlişkin Kafa Karıştıran 6 Konu ve Bunlara İlişkin Yorumlar**, http://bertankaya.net/index.php/2014/07/ic-denetime-iliskin-kafa-karistiran-6-konu-ve-bunlara-iliskin-yorumlar/, (01.04.2017).

Kaya, Bertan, (2014), **İç Kontrolün Özü Nedir**, http://bertankaya.net/?p=1104, (02.02.2017).

Kaya, Bertan, (2011), **İşe Nereden Başlamalı: İç Denetim İç Kontrol veya Risk Yönetimi**, http://bertankaya.net/?p=498, (09.01.2017).

Kaya, Bertan, (2015), **Risk Yönetim Planı Nasıl Oluşturulur**, http://bertankaya.net/?p=1104, (02.02.2017).

Kızılboğa, Ruveyda, (2012), ‘‘Geleneksel Risk Yönetiminden Kurumsal Risk Yönetim Sistemine Geçiş’’, **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, S.16(3): 297-316, s. 306.

Kızılboğa, Ruveyda, (2013), **Kurumsal Risk Yönetimi Odaklı İç Denetim ve İstanbul Büyükşehir Belediyesi İçin Bir Model Önerisi**, İstanbul: Marmara Belediyeler Birliği Yayını, S.76, s. 70.

KPMG, (2015), **Risk Assesment**, COSO Framework, https://www.isaca.org/chapters1/phoenix/events/Documents/KPMG-COSO Presentation.pdf, (28.10.2017).

Lark, Kate, Walker, Paul L., (2008), **Risk Management, Enterprise Risk Management**, http://docplayer.net/11852964-Rims-risk-management-models-traditional-risk-management-progressive-risk-management-strategic-risk-management.html (01.11.2017).

Moller, Robert R., (2005), **Brink’s Modern Internal Auditing**, John Wiley & Sons,

Özbek, Çetin, (2012), **İç Denetim**, 1. Baskı, Yayın No: 3, İstanbul: Türkiye İç Denetim Enstitüsü Yayınları, C.1, s. 3-400.

Pehlivanlı, Davut, (2014), **Modern İç Denetim**, 2. Baskı, İstanbul: Beta Yayınları.

PricewaterhouseCoopers Türkiye Danışmanlık Hizmetleri, **Her Yönüyle Kurumsal Risk Yönetimi**, http://docplayer.biz.tr/370845-Her-yonuyle-kurumsal-risk-yonetimi.html, (10.12.2017).

Protiviti, (2006), **Guide To Enterprise Risk Management**, Frequently Asked Questions, http://www.ucop.edu/enterprise-risk-management/_files/protiviti_faqguide.pdf, (06.09.2017).

Protiviti, (2014), **The Updated COSO Internal Control Framework**, Frequently Asked Questions, Third Edition, https://www.protiviti.com/sites/default/files/united_states/insights/updated-coso-internal-control-framework-faqs-third-edition-protiviti.pdf, s. 27, (15.07.2017).

Rittenberg, L., Martens, F., **Understanding And Communicating Risk Appetite**, COSO Enterprise Risk Management, https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf, (12.11.2017).

Rubin, Ken, (2014), **Agile & Risk Management**: **The Role of Traditional Risk Management**, http://www.innolution.com/blog/agile-risk-management-the-role-of-traditional-risk-management, (08.06.2017).

Saka, T., Uğural, A., (2014), **Kurumsal Risk Yönetimi**, http://tusiad.org/tr/tum/item/download/2466_aff40c11210dd71986e25302c58160ca, s. 22, (15.05.2017).

Topçu, Bünyamin, (2012), ‘‘İşletmelerde Kurumsal Risk Yönetimi’’, **İstanbul Ticaret Odası Yayınları**, İstanbul, http://www.ito.org.tr/itoyayin/0015264.pdf, S.27, s. 25, (13.09.2017).

Tüm, Kayahan, (Aralık 2013), ‘‘Kurumsal Yönetim İç Denetim ve İç Denetimin Kalitesi: Kalite Güvence ve Geliştirme Programı’’, **Çukurova Üniversitesi İİBF Dergisi**, C.17, S.2, s. 93-112, http://dergipark.ulakbim.gov.tr/cuiibfd/article/view/5000136769/5000125669, (03.10.2017).

Türkiye Cumhuriyeti Maliye Bakanlığı, İç Denetim Koordinasyon Kurulu, **Kamu İç Denetim Terimler Sözlüğü**, http://www.idkk.gov.tr/Sayfalar/Mevzuat/Ucuncul%20Duzey%20Mevzuat/KamuIcDenetimTerimleriSozlugu.aspx, (19.11.2017).

Türkiye İç Denetim Enstitüsü, ‘‘Kurumsal Yönetimin Güvencesi İç Denetim’’, **Platin Dergisi Eki**, https://www.tide.org.tr/uploads/news/Platin_Ek.pdf, s. 3-6, (03.03.2017).

Türkiye Kurumsal Yönetim Derneği, http://www.tkyd.org/tr/sss-kurumsal-yonetim-ilkeleri-nedir.html, (15.09.2017).

Türk Sanayicileri ve İş Adamları Derneği (TÜSİAD), (2008), ‘‘Kurumsal Risk Yönetimi’’, **TÜSİAD Yayınları**, Yayın No: TÜSİAD-T/2008-02/452, http://tusiad.org/tr/yayinlar/raporlar/item/download/3470_3def5dc2dc47e5faf697ba2bcb541181, s. 19-20, (25.09.2017).

Uluslararası İç Denetçiler Enstitüsü, **Ana Prensipler**, Uluslararası Mesleki Uygulama Çerçevesi, Türkiye İç Denetim Enstitüsü (Çev.), http://www.tide.org.tr/page.aspx?nm=Ana_Prensipler, (23.10.2017).

Uluslararası İç Denetçiler Enstitüsü, **Etik Kurallarıyla Tanışma Metni**, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/page.aspx?nm=EtikKurallari#etkurtan, (19.11.2017).

Uluslararası İç Denetçiler Enstitüsü, (2013), **Etkili Risk Yönetimi ve Kontrolünde Üç Savunma Hattı**, Görüş Açıklamaları, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/PP_3_Savunma_Hatti.pdf, (19.02.2017).

Uluslararası İç Denetçiler Enstitüsü, **İç Denetim Güvence İçgörü Nesnellik**, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/news/IIA_Ic_Denetimin_Paydaslar_Icin_Degeri_Detay.pdf, (04.05.2017).

Uluslararası İç Denetçiler Enstitüsü, (2012), **İç Denetimin Katma Değeri ve Kapasite Modeli**, Ek Rehber, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/SG_Ic_Denetimin_Katma_Degeri.pdf, (01.03.2017).

Uluslararası İç Denetçiler Enstitüsü, (2009), **İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol**, Uluslararası Mesleki Uygulama Çerçevesi, Pozisyon Raporu, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/PP-KRY_de_Ic_Denetimin_Rolu.pdf, (02.02.2017).

Uluslararası İç Denetçiler Enstitüsü, **İç Denetimin Paydaşlar İçin Değeri**, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/news/IIA_Ic_Denetimin_Paydaslar_Icin_Degeri.pdf, (05.02.2017).

Uluslararası İç Denetçiler Enstitüsü, (Temmuz 2009), **İç Denetim Planlamasında Risk Yönetim Süreçlerinin Kullanılması**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Önerisi 2010- 2, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/, (21.02.2017).

Uluslararası İç Denetçiler Enstitüsü, (Temmuz 2015), **Kurumsal Yönetim**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Rehberi 2110, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/, (06.05.2017).

Uluslararası İç Denetçiler Enstitüsü Norge (Norveç), (2017), **Guidelines For The Risk Management Function**, http://iia.no/wp-content/uploads/2017/05/2017-Guidance-for-the-Risk-Management-Function.pdf, s. 7, (04.10.2017).

Uluslararası İç Denetçiler Enstitüsü, (Temmuz 2012), **Özel Sektörde Kurumsal Yönetişimin Değerlendirilmesi**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Rehberi, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/PG-Ozel_Sektorde_Kurumsal_Yonetisim.pdf, (18.04.2017).

Uluslararası İç Denetçiler Enstitüsü, (Aralık 2016), **Risk Yönetimi**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Rehberi 2120, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/, (16.04.2017).

Uluslararası İç Denetçiler Enstitüsü, (Mart 2012), **Risk Yönetimi ve Güvence Görevlerinin Koordinasyonu**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Rehberi, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/, (09.09.2017).

Uluslararası İç Denetçiler Enstitüsü (IIA), (2017), **Standartlar,** Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ) Kapsamında Uluslararası İç Denetim Standartları (Standartlar), Revizyon Tarihi: Ekim 2016 - Geçerlilik Tarihi: Ocak 2017, Türkiye İç Denetim Enstitüsü (Çev.), http://www.tide.org.tr/uploads/UMUC-2017-updated.pdf, s. 1-29, (15.11.2017).

Uluslararası İç Denetçiler Enstitüsü, **Standartlarla Tanışma Metni**, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/uploads/pdf/StandartlarlaTanismaMetni.pdf, (19.11.2017).

Uluslararası İç Denetçiler Enstitüsü, **Uluslararası Mesleki Uygulama Çerçevesi**, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/page.aspx?nm=umuc, (04.06.2017).

Uluslararası İç Denetçiler Enstitüsü, (2015), **YENİ International Professional Practice Framework (IPPF)**, Türkiye İç Denetim Enstitüsü (Çev.), http://www.tide.org.tr/uploads/IPPF-Toolkit-Copy-Flyer-and-Ad%2029072015.pdf, (17.11.2017).

Uluslararası İç Denetçiler Enstitüsü, (Nisan 2010), **Yönetişim: Risk ve Kontrol ile İlişki**, Uluslararası Mesleki Uygulama Çerçevesi, Uygulama Önerisi 2110: 2, Türkiye İç Denetim Enstitüsü (Çev.), https://www.tide.org.tr/, (04.03.2017).

Uwadiae, Oduware, Deloitte, ‘‘COSO An Approach to Internal Control Framework’’, **Financal Reporting Deloitte**, https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/audit/Financial%20Reporting/ng-coso-an-approach-to-internal-control-framework.pdf, (10.12.2017).

Uyar, Süleyman, (2009), **İç Kontrol ve İç Denetim**, Ankara: Gazi Kitabevi.

Uzun, Ali Kamil, **İç Denetim Nedir**, Deloitte Türkiye, http://www.denetimnet.net/UserFiles/Documents/Makaleler/%C4%B0%C3%A7%20Denetim/%C4%B0%C3%A7%20Denetim%20Nedir-Makale.pdf, (06.11.2017).

W., Stippich, Warren, (2015), **The 4 Risk Assessment Principles of The 2013 COSO Framework**, Principle 7: Identify And Analyze Risks Across The Entity, http://www.corporatecomplianceinsights.com/the-4-risk-assessment-principles-of-the-coso-framework/, (17.09.2017).

WU, Yan, (2015), **Enterprise Internal Control From the Perspective of Risk Management**, Jilin Business and Technology College, Changchun City Jilin Province, China, http://download.atlantis-press.com/php/download_paper.php?id=7314, s. 705, (20.11.2017).

Yurtsever, Gürdoğan, (2015), ‘‘İç Denetimin Fonksiyonları ve Katma Değeri’’, **Finans Politik & Ekonomik Yorumlar**, www.ekonomikyorumlar.com.tr/dergiler/makaleler/602/sayi_602_makale-06.pdf, C.52, S.602, s. 90, (04.08.2017).

http://arsiv.ntv.com.tr/news/160390, (20.11.2017).

https://global.theiia.org/Pages/globaliiaHome.aspx, (17.10.2017).

https://ipfs.io/ipfs/QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Risk_analizi.html, (16.09.2017).

https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx, (09.12.2017).

https://na.theiia.org/Pages/IIAHome.aspx, (21.07.2017).

https://tez.yok.gov.tr/UlusalTezMerkezi/, (01.04.2017).

https://www.tide.org.tr/, (12.10.2017).

https://www.tide.org.tr/page.aspx?nm=PozisyonRaporlari, (06.12.2017).

https://www.pwc.com.tr/tr/hizmetlerimiz/denetim/sarbanes-oxley.html, (29.11.2017).

www.businessalignment.weebly.com/home/2921559, (01.11.2017).

www.commsrisk.com/new-coso-erm-framework-out-for-comment/, (11.11.2017).

www.controlsframework.com/info_communication.php, (25.09.2017).

www.controlsframework.com/monitoring.php, (12.11.2017).

www.coso.org/, (05.05.2017).

www.coursehero.com/file/p2mr1kv/ACC-444-Enterprise-Process-Analysis-27-RISK-ASSESSMENT-AND-RISK-RESPONSE-COSO/, (03.10.2017).

www.eurocert.com.tr/iso-31000-risk-yonetimi.aspx, (06.12.2017).

www.iaaglobal.org/, (05.08.2017).

www.iia.org.uk/, (12.09.2017).

www.isaca.org/Journal/archives/2013/Volume-4/Pages/Key-Elements-of-an-Information-Risk-Profile.aspx?utm_referrer=, (10.09.2017).

www.moresecure.ca/risk-management, (02.10.2017).

www.theirm.org/media/1001360/SARMERMPublishFinal14Feb2012.pdf, (05.10.2017).

www.theirm.org/the-risk-profession/risk-management.aspx, (16.09.2017).

GENEL BİLGİLER

İsim ve Soyadı	:	Caner ERŞAN
Anabilim Dalı	:	İşletme
Tez Danışmanı	:	Yrd. Doç. Dr. Özgür ATEŞ
Tez Türü ve Tarihi	:	Yüksek Lisans - Şubat 2018
Anahtar Kelimeler	:	İç Denetim, Risk Yönetimi, Kontrol, Kurumsal Yönetim.

ÖZET
İÇ DENETİM ALANINDA RİSK YÖNETİMİNİN KAVRAMSAL ANALİZİ

IIA'ya göre iç denetim: ''Bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir.'' ve odak noktasını: *''Risk Yönetimi'', ''Kontrol'' ve ''Kurumsal Yönetim''* süreçleri oluşturur. İç denetim alanında risk yönetiminin kavramsal boyutunu ve önemini belirlemek için, risk yönetimi ile bu kavramlar arasındaki etkileşim ağının analiz edilmesi gerekir. Aralarında güçlü ilişkiler barındıran bu kavramların analiz edilmesi; soyut risk yönetim kavramlarının zihinlerde somutlaştırılmasına, ortak bir çerçevede algılanmasına ve risk yönetim faaliyetlerinin etkinliğinin arttırılmasına katkı sağlayacaktır.

Risk yönetimi geniş bir literatür ve uygulama yelpazesine sahiptir, bu yüzden risk yönetiminde farklı anlayışlar ve değerlendirmeler yapılabilir. İç denetimin kapsamı; risk yönetimi, yönetişim ve kontrol süreçleri ile ilgilidir, bu nedenle bu çalışma iç denetim kapsamında sadece risk yönetiminin kavramsal analizini içermektedir. COSO ve IIA tarafından yayınlanan belgeler, bu çalışmanın temel felsefesini oluşturmuştur.

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

GENERAL KNOWLEDGE

Name and Surname	:	Caner ERŞAN
Field	:	Business Administration
Supervisor	:	Assistant Prof. Özgür ATEŞ
Degree Awarded and Date	:	Master - February 2018
Key Words	:	Internal Auditing, Risk Management, Control, Governance.

ABSTRACT
CONCEPTUAL ANALYSIS OF RISK MANAGEMENT IN THE FIELD OF INTERNAL AUDITING

According to IIA, Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations and it focus on: *''Risk Management,'' ''Control'' and ''Governance''* processes, to determine the conceptual dimension and importance of risk management in the field of internal auditing, the interaction network among risk management and these concepts needs to be analyzed. Analyzing these concepts which have strong relations among them will contribute to embody the concepts of abstract risk management in minds, to be perceived in a common framework and to increase the effectiveness of risk management activities.

Risk management has a wide range of literatures and practices therefore there can be different understandings and assessments in risk management. The scope of internal auditing is related to the risk management, governance and control processes so this study included just conceptual analysis of risk management within the scope of internal auditing. The documents published by COSO and IIA point of view constituted the basic philosophy of this study.

Key Words: Internal Auditing, Risk Management, Control, Governance.