Sosyal Bilimler Enstitüsü

T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

MUHASEBE-FİNANSMAN BİLİM DALI

KURUMSAL RİSK YÖNETİMİ SÜRECİNİN İÇ DENETİMİ VE BİR ARAŞTIRMA

Doktora Tezi

MÜGE MERT KÖRÜK

İstanbul, 2024

T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

MUHASEBE-FİNANSMAN BİLİM DALI

KURUMSAL RİSK YÖNETİMİ SÜRECİNİN İÇ DENETİMİ VE BİR ARAŞTIRMA

Doktora Tezi

MÜGE MERT KÖRÜK

Tez Savunma Jürisi

1.Tez Danışmanı: Prof. Dr.Nuran Cömert

2. Üye: Prof. Dr.Doğan Argun

3. Üye: Prof. Dr.Duygu Anıl Keskin

4. Üye: Prof. Dr.Fatma Lerzan Kavut

5. Üye: Doç. Dr.Mehmet Nuri İnel

İstanbul, 2024

ÖZET

KURUMSAL RİSK YÖNETİMİ SÜRECİNİN İÇ DENETİMİ VE BİR ARAŞTIRMA

İşletmelerin stratejilerini gerçekleştirmelerine, hedeflerine ulaşmalarına en çok destek olan erken tanı (teşhis) sistemi risk yönetimi sürecidir. Zamanla pazar koşullarının değişmesi, rekabetin artması ve yaşanan ekonomik, teknolojik gelişmeler sonucunda risk yönetimi kavramı kurumsal risk yönetimi anlayışına dönüşmüştür. Bu anlayış, işletmelerin faaliyetlerini sürdürebilmesini tehdit altına alacak tüm riskleri ve işletmeyi hedeflerine yaklaştıracak tüm fırsatları bütünleşik (entegre) bir ortamda ve sistematik olarak yönetmeyi amaçlamaktadır. Önetkin (proaktif) bakış açısını da beraberinde getiren kurumsal risk yönetimi yaklaşımı, iç denetime de önemli misyonlar yüklemiştir. İç denetimin, güvence ve danışmanlık rolleri kapsamında yürüteceği kurumsal risk yönetimi (KRY) odaklı denetim sayesinde hem KRY sürecine hem de işletmeye katma değer yaratacağı çok açıktır. İç denetim, kurumsal risk yönetimi uygulamalarında önemli rol oynar ve aynı zamanda kurumsal risk yönetimi süreçlerinin varlığı, doğru uygulanıp uygulanmadığını inceler. Bu kapsamda, risk raporlama çeşitlerinin ve içeriğinin kontrolünü yapar, süreçteki tüm eşgüdümü denetler. İç denetçiler risk yönetim süreçlerinin denetimiyle ilgili olarak işletmeye hem güvence hem de danışmanlık hizmeti verebilirler.

Bu çalışmada KRY sürecinin işleyişi ve bu işleyişin iç denetçiler tarafından denetimi, konuyla ilgili önemli çerçeveler ve standartlar temel alınarak incelenmiş, ülkemizde kurumsal risk yönetimi uygulamalarında iç denetimin etkililiği ve rolü üzerine BIST-50 şirketlerinde nicel analiz yöntemlerinden biri olan keşifsel araştırma yöntemi kullanılarak bir araştırma yapılmış ve bu araştırma kapsamında Türkiye'nin kurumsallaşma anlamında önde gelen şirketlerinde iç denetimin KRY olgunluk düzeyine ne ölçüde katkıda bulunduğu anlaşılmaya çalışılmıştır.

Anahtar Kelimeler: Risk, Fırsat, Risk Yönetimi, Kurumsal Risk Yönetimi, İç Denetim, COSO KRY.

ABSTRACT

INTERNAL AUDITING OF ENTERPRISE RISK MANAGEMENT PROCESS AND AN EMPIRICAL STUDY

Risk management system is an early warning system that provides companies to reach their targets and achieve their strategies. Due to change in market conditions, increase in competition and ongoing economic and technological developments the concept of risk management has evolved into the understanding of enterprise risk management (ERM). This approach aims to systematically manage all risks that threaten the continuity of business operations and all opportunities that bring the business closer to its goals in an integrated and systematic environment. ERM which brings a proactive perspective, has also assigned significant missions to internal auditing. It is very clear that through ERM-focused audits conducted under assurance and consultancy roles, value will be added to both the ERM process and business. Internal auditing plays an important role in enterprise risk management practices and also examines whether the ERM processes are available and implemented correctly. In this context, it controls the types and content of risk reporting and oversees all coordination in the process. Internal auditors can provide both assurance and consultancy services to the business regarding internal audit of risk management processes.

In this study, the functioning of the ERM process and its internal audit are examined based on important frameworks and standards related to this subject. An empirical study was conducted through a survey on in Turkey's leading companies (BIST-50 companies) to investigate the effectiveness and role of internal audit in enterprise risk management practices. Within the scope of this study, an analysis/research has been made to understand the contribution of internal audit to the ERM maturity level in Turkey's leading companies in terms of institutionalization.

Key Words: Risk, Opportunity, Risk Management, Enterprise Risk Management, Internal Audit, COSO ERM Framework.

ÖNSÖZ

Tez çalışmamda değerli görüşleri ve geri bildirimleriyle teze katkıda bulunan ve üzerimde uzun yıllardır çok emeği olan saygıdeğer hocam ve tez danışmanım Sayın Prof. Dr. Nuran Cömert'e, çalışmanın şekillenip tamamlanması sürecinde kıymetli görüşlerini esirgemeyen saygıdeğer hocalarım Sayın Prof. Dr. Doğan Argun ve Sayın Prof. Dr. Duygu Anıl Keskin'e, tez savunma jürisinde bulunarak değerli katkılarıyla tezin son halini almasını sağlayan saygıdeğer hocalarım Prof. Dr. Fatma Lerzan Kavut'a ve Doç.Dr. Mehmet Nuri İnel'e sonsuz teşekkürlerimi ve saygılarımı sunarım.

Hayatımın her döneminde sevgilerini, desteklerini eksik etmeyen canım anneme, babama, kaybettiğim kıymetli eşim Egemen'e teşekkür eder, çalışmanın tüm ilgililere yararlı olmasını dilerim.

Müge MERT KÖRÜK

İstanbul, 2024

İÇİNDEKİLER

KISALTMALAR

AAA	Amerikan Muhasebe Kurumu
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AICPA	Amerikan Yetki Belgeli Muhasebeciler Enstitüsü
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BIST	Borsa İstanbul
BT	Bilgi Teknolojileri
CIA	Sertifikalı İç Denetçi
COSO	Treadway Komisyonu (The Committee of Sponsoring Organizations)
ERM	Enterprise Risk Management
FEI	Uluslararası Finansal Yöneticiler
GTAG	Global Teknoloji Denetim Rehberleri
ICAEW	Institute of Chartered Accountants in England and Wales
IIA	İç Denetçiler Enstitüsü
IMA	Yönetim Muhasebesi Enstitüsü
INTOSAI	Uluslararası Yüksek Denetim Kurumları Teşkilatı
IPPF	Uluslararası Mesleki Uygulamalar Çerçevesi
ISACA	Bilgi Sistemleri Denetim ve Kontrol Birliği
ISO	Uluslararası Standartlar Teşkilatı
KonTrag	Alman İş Hayatında Kontrol ve Şeffaflık Yasası
KRY	Kurumsal Risk Yönetimi
Md	Madde

OECD	Organisation for Economic Co-Operation and Development
PCAOB	Halka Açık Şirketler Kamu Muhasebe Gözetim Kurulu
RIMS	Risk Yönetimi Topluluğu
SEC	Birleşik Devletler Menkul Kıymetler ve Borsa Komisyonu
SOX	Sarbanes Oxley Yasası
SPK	Sermaye Piyasası Kurulu
SWOT	Zayıf Yönler, Güçlü Yönler, Tehditler, Fırsatlar (Weaknesses, Strenghts, Threats, Oppotunities)
TİDE	Türkiye İç Denetim Enstitüsü
TKYD	Türkiye Kurumsal Yönetim Derneği
TMS	Türkiye Muhasebe Standartları
TTK	Türk Ticaret Kanunu
TÜSİAD	Türk Sanayicileri ve İş İnsanları Derneği
UMUÇ	Uluslararası Mesleki Uygulamalar Çerçevesi

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

1. GİRİŞ

Günümüzde toplumların ihtiyaç duyduğu işletmeler; adil, sorumlu, şeffaf ve hesap verebilir bir anlayışla yönetilen işletmelerdir. İyi yönetişim (good governance) olarak ifade edilen bu yönetim anlayışında işletmelerin risk temelli etkili bir iç kontrol sistemi ve bu işleyişi destekleyen iyi bir kurumsal risk yönetim süreci kurmaları ve kurdukları bu yapıyı da sürekli gözeten mekanizmaları oluşturmaları beklenir. Kurumsal misyona ve vizyona uygun kurumsal planlarla hedefler oluşturulup iyi bir kaynak dağılımı ile işletmenin bütün unsurları harekete geçirilirken tüm faaliyetlerin, yasal gerekliliklerin ve raporlama sorumluluklarının uygun şekilde yerine getirilip getirilmediğinin gözetimi ve denetimi gereklidir. Dünya genelinde kabul gören kurumsal yönetim ilkeleri, işletme yönetimlerine gerek iyi yönetişim gerek risk yönetimi, gerekse iç kontrol sistemlerinin denetimi konusunda bağımsız konumda ve tarafsız bir zihniyetle çalışan bir iç denetim birimi kurmalarını önermektedir. OECD'nin (Organisation for Economic Co-Operation and Development) kurumsal yönetim ilkeleri ülkemizin de altına imza attığı ve ülkemizde kamuya hesap verme sorumluluğu olan işletmeleri bağlayıcı özelliği de olan en önemli rehberlerden bir tanesidir. (OECD, Kurumsal Yönetim İlkeleri Rehberi, V. Bölüm, 2023)

Diğer yandan Amerika Birleşik Devletleri'nde (ABD) giderek artan sayıda Enron, WorldCom, Sunbeam, Tyco gibi şirket skandalları, finansal tablo manipülasyonları dikkatin başarısız yöneticilere çevrilmesine ve yöneticilerin sorumluluklarının sorgulanmasına sebep olmuştur. Bu süreçte ilk kez 1985 yılında hileli finansal raporlamayı önlemek amacıyla beş mesleki kuruluşun (sponsor kuruluşların) bir araya gelerek oluşturduğu ve milli olarak nitelendirdikleri COSO (Orijinal adı (Treadway Komisyonu) 1992 yılında yönetimleri sorumlu tutmada rehber alınacak bir çerçeve yayınlamıştır. ***İç Kontrol-Bütünleşik Çerçeve*** başlıklı bu çerçeve, Amerikan halka açık şirket yönetimlerine dürüst işleyen etkili iç kontroller kurma, işletme ve sorumluluğunu üstlenme konusunda yeni yükümlülükler getiren Sarbanes Oxley (SOX) Yasasında referans alınmıştır. 2013 yılında güncellenen söz konusu çerçeve sponsor kuruluşların etkisiyle giderek dünya genelinde de rehber alınan önemli bir çerçeve haline gelirken, COSO, kendini oluşturan beş mesleki örgütün *–Amerikan Muhasebe Kurumu(AAA), Amerikan Yetki Belgeli Kamu Muhasebeciler Enstitüsü (AICPA), Uluslararası Finansal Yöneticiler (FEI), Uluslararası İç Denetçiler Enstitüsü (IIA) ve Yönetim Muhasebecileri Enstitüsü (IMA) olarak bilinen Ulusal Muhasebeciler Enstitüsü* - her birinden tamamen bağımsız bir şekilde çalışan bir düşünce kuruluşuna dönüşmüştür. COSO'nun

Günümüzde, ***İç Kontrol, Kurumsal Risk Yönetimi, Hilenin Önlenmesi ve Yönetişimi*** konularında hazırladığı çerçevelerin her biri ülkemiz de dahil olmak üzere dünya genelinde itibar edilen bir kalite rehberi olarak kabul görmektedir. Zamanla işletmelerin ihtiyaçlarının değişmesinin de etkisiyle, COSO 2017 yılında kurumsal risk yönetimi çerçevesini "Riskin Strateji ve Performansla Uyumlaştırılması" ismi ile güncellemiştir.

Bütün bu gelişmeleri takiben COSO'nun en etkili sponsor kuruluşlarından biri olan Uluslararası İç Denetçiler Enstitüsü, 1990'lı yılların sonunda yeni bir iç denetim tanımı yaparak iç denetim ilke ve standartlarında önemli bir değişikliğe gitmiş iç denetimin değer yaratan proaktif rolünü öne çıkaran ve kırmızı kitap diye anılan Uluslararası Mesleki Uygulamalar Çerçevesini (IPPF 2002) yayınlamıştır. (Sridhar. R. 2003: 2-6) İç denetimin devrim yaratan yeni tanımı yanında denetçiler için etik ilke ve kurallar ile birlikte iç denetçilerin niteliksel özellikleri ve iç denetim faaliyetinin yönetimi ve yürütülmesi için standartlar içeren bu çerçeve iç denetim birimini yasal olarak kurmak zorunda sermaye piyasası kurum ve kuruluşları için uyulması zorunlu kurallara dönüşmüştür. İç Denetimin bu yeni tanımı iç denetçiye bağımsız ve tarafsız konumda üç görev alanı öngörmüştür. Yönetişim süreçleri, risk yönetim süreçleri ve iç kontrollerin etkililiğinin değerlendirilmesi olarak öngörülen bu denetim konularında iç denetçiler işletmelerin yönetim kurullarına güvence ve danışmanlık hizmeti verebilmektedirler.

Gerek ülkemizde gerek dünyada diğer ülkelerde yasal düzenlemeler, kamuya hesap verme sorumluluğu olan ya da kamu yararını ilgilendiren, özellikle para ve sermaye piyasalarında faaliyet gösteren kurum ve kuruluşlarda hem iç denetim birimlerinin hem de risk yönetim birimlerinin kurulmasını ve bu birimlerin her ikisinin birden fonksiyonel olarak en tepe yönetime, genellikle de yönetim kuruluna bağlı olmasını öngörmektedir. Esasen bu durum yönetim kurulu adına işletmenin risk yönetim süreçlerinin etkililiğini değerlendirmek zorunda olan iç denetçinin bağımsızlığına ve tarafsızlığına zarar verebilecek bir örgütsel çatışmayı da beraberinde getiren bir probleme işaret edebilmektedir.

Bu çalışmanın temel amacı, işletmelerde kurumsal risk yönetimi (KRY) ve iç denetimin ilişkisini ve etkileşimini incelemek, bu konuyla ilgili dünya genelinde kabul gören çerçeveleri (rehberleri) temel alarak kurumsal risk yönetimi sürecinin işletmelerde nasıl işletildiği ve denetlendiğini ve aynı bağlamda KRY sürecinin etkililiği konusunda iç denetimin kime nasıl güvence verdiğini, süreçte nasıl rol ve sorumluluklar üstlendiğini ortaya koymaktır.

Bu amaçla tezimizde öncelikle önemli bulduğumuz genel kavramlar ile iyi bir KRY sürecinde olması gerekenleri belirleyebilmek için dünyada rehber alınan genel çerçeveler ele alınarak açıklanmış ardından tez konumuzla ilgili öncül nitelikte olabilecek çalışmalar olup olmadığının tespiti için yok.gov.tr ulusal tez merkezi başta olmak üzere bir literatür taraması yapılmıştır. Bu çalışmaları takiben iç denetimin KRY sürecini nasıl denetlediği ve söz konusu süreçteki rol ve sorumluluklarını etkili bir şekilde yerine getirip getirmediği konusu incelenmiştir. İncelememizle ilgili önce teorik bilgiler ve geçerli uygulama standartları açıklanmış daha sonra hem iç denetim birimi hem de KRY sistemi kurmak zorunda olmaları sebebiyle BIST-50 şirketlerindeki uygulamalara ilişkin bir araştırma yapılmıştır. Ülkemizde BİST 50'de yer alan şirketlere yönelik olarak yapılan araştırmada nicel analiz yöntemlerinden biri olan keşifsel araştırma yöntemi kullanılmıştır.

2. RİSK KAVRAMI, RİSK YÖNETİMİNE ve KURUMSAL YÖNETİME GENEL BAKIŞ

2.1. Risk Kavramı

Risk kelimesi, Fransızca kökenli olup, kelimenin aslı "riziko"dur. Risk kelimesinin altında herhangi bir karar verme anında gelecekteki olaylar hakkında net bilgilere sahip olmamak yatmaktadır. (Özbilgin, G. 2012: 88)

Risk kavramı, beklenmeyen bir olayın işletmeye olan tahmini etkilerinin tamamını ifade etmektedir. Risk sözcüğü, İtalyanca'daki "riscare" kelimesinden gelmekte ve "cesaret etmek" anlamında kullanılmaktadır. Başka bir ifadeyle, risk beklenen durumda meydana gelen sapmanın işletmenin hedefleri üzerindeki olumsuz etkisidir. Bu noktada oluşan sapma işletmeye olumlu etki ediyorsa bu da fırsat veya şans kavramı ile tanımlanmaktadır. Risk kelimesinin Çince karşılığının fırsat anlamına gelmesi de oldukça dikkat çekicidir. (Bakkal, Tunç, Kasımoğlu, 2016:37) Uluslararası İç Denetçiler Enstitüsü (IIA) ise riski; "İşletmenin hedeflerine ulaşmasını etkileyebilecek bir olayın oluşmasına dair bir belirsizlik" olarak tanımlamaktadır. İşletmeler, hedeflerine ulaşmalarına engel olabilecek potansiyel durumları önceden öngörmek ve bu konulara dair önlemler almakla sorumludurlar. Dolayısıyla risklerin/fırsatların yönetimi, işletmenin hem sürdürülebilirlik ile ilgili bir amacıdır hem de erken uyarı sistemi içindeki en önemli görevlerinden biridir.

Karar alma süreçlerinde, öncelikle kararın güvenli bir ortamda mı güvensiz bir ortamda mı alındığı çok önemlidir. Güvenli durumlarda bir kararın sonucu tamamen belirlenmiş gibidir. Ancak gerçekte neredeyse tamamen belirsizlik vardır; yani bir kararın, karar anında hangi sonuca ulaşılacağı açık değildir ve farklı sonuçları olabilmektedir. (Oehler, Unser, 2002:10)

Risklerin tanımlanması esnasında, risk algısı da kapsama girmektedir. (Sha, 2001: 348)

Risk yönetimi sürecinde riskin algılanması konusunda belirleyici olan faktörlerden bazıları aşağıda ifade edilmiştir: (Schmidt, 2004: 3)

• **İhtiyarilik:** Bir olayda ihtiyarilik sözkonusu ise, doğal olarak bu durumda o olayın risk olarak algılanma ihtimali düşecektir. Eğer olayda zorunluluk varsa, bu noktada risk algısının yükselmesi muhtemeldir.

- **Kontrol Edilebilirlik**: Algılanan mevcut riskler işletmenin kontrolünde ise bu risklerin kabul edilme olasılığı yüksektir. Genelde çalışanlar kendi kontrolleri altında olmayan riskleri kabullenmekte zorlanırlar.
- **Gecikme Etkisi:** Bir olayın gerçekleşmesi ile etkisinin oluşması arasında bir zaman farkı olabilir. Bu gecikmenin varlığı, riskin belirlenmesinde de muğlaklık yaratarak zorluk çıkmasına sebep olur. Örneğin, insan vücuduna zararlı maddeleri tüketmenin etkileri yıllar sonra görülmektedir. Bu nedenle kişiler bu durumda riski algılamakta ve önlem almakta zorlanmaktadırlar.
- **Aşinalık ve Alışkanlık:** Detaylarına hakim olunan riskler, belirsiz tarafların çok bulunduğu risklere göre çok daha kolay algılanıp kabul edilebimektedir. Ancak kabul edilmiş ve uzun süredir devam eden riskler de de riske aşina olma sonucunda konu bir alışkanlık haline gelmektedir.

Riskler yönetilebildiği sürece hayatın olağan akışında esaslı bir sorun teşkil etmezler. Ancak, hayatın içinde risklerle baş etme becerimiz ile maruz kaldığımız riskler arasında orantısız bir büyüme mevcuttur.

Amerika'da kontrol risk yönetimi, yönetişim ve hile önleme konularında düşünce liderliği yapan bir kuruluş olan COSO, riski -sonraki bölümlerde de anlatılacağı üzere- "İşletmelerin geleceğini tehdit altına sokabilecek her türlü olay" olarak tanımlanmıştır.

Risk kavramı, içeriği itibariyle belirsizlik, olasılık temalarıyla yakından ilgilidir ve bu konularla beraber değerlendirilmedir.

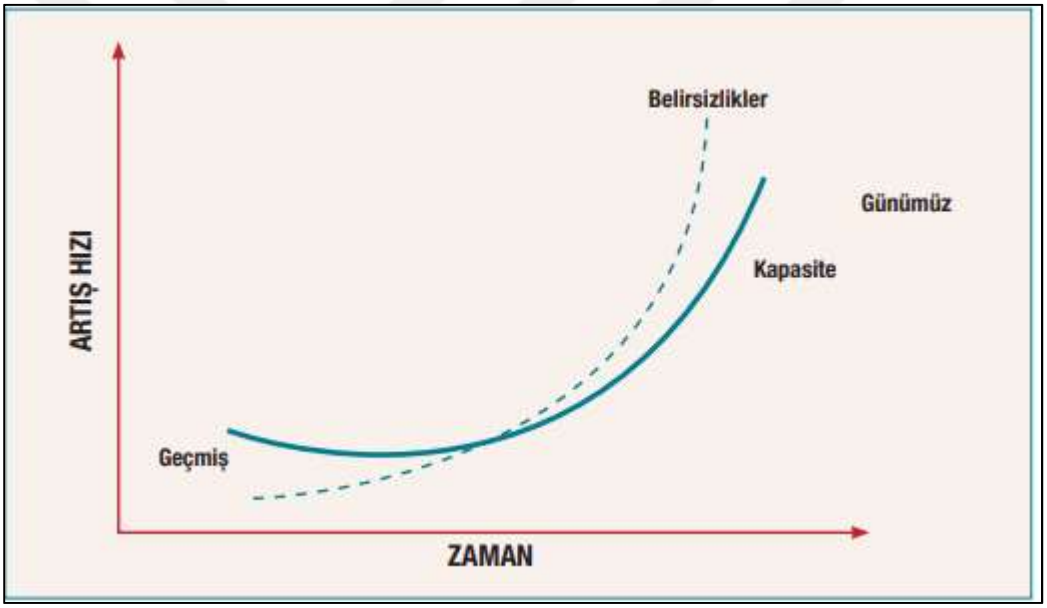
Frank Night, risk ve belirsizlik arasındaki ilişkiyi "Riskin ölçülebilmesi durumunda risk olarak adlandırılması, ölçülüp sayılarla ifade edilememesi halinde belirsizlik olarak tanımlanması" gerektiğini belirtmiştir. (Knight, F.H. 1921) Riskin tanımlanabilmesi için bir belirsizliğin olması ve bu belirsizliğin bir zarara yol açması gerekir. Öncelikle yapılması gereken şey, riskin gerçekleşme olasılığının hesaplanması ve bundan sonra da işletmeye vereceği zararın sayılarla ifade edilmesidir. Aksi durumda, eğer risk sayısal şekilde ifade edilemiyorsa o zaman onu risk olarak değil belirsizlik olarak tanımlamak daha doğru olacaktır. (Özbek, 2012:236)

Risklerin barındırdığı belirsizlik ortamı bir kayba yol açabileceği gibi aynı zamanda fırsatlar da doğurabilmektedir. İşte bu noktada etkili risk ve fırsat yönetimi gündeme gelmektedir. Riskler olduğu kadar fırsatlar da tanımlanmalı, ölçülüp değerlendirilmeli ve uzun dönemli olarak takip edilmelidir. Risk ve fırsatın birbirini tamamlayan unsurlar olduğu hiçbir zaman unutulmamalıdır.

Maruz kalınan belirsizlikler, sonuçları itibariyle önemli olanlar ve önemli olmayanlar olarak iki başlık altında toplanmaktadır. Hangi belirsizliklerin önemli olduğu hangilerinin önemsiz olduğuna ilişkin değerlendirilmesi gereken husus ise, süreçteki amaçtır. Bu yönüyle de risk, gerçekleşmesi halinde amaçlara erişilmesine olumlu ya da olumsuz etkisi olan belirsizliktir.

İstatistiksel olaylar risk taşırken, istatistiksel olmayan olaylar belirsizlik taşımaktadır. Ayrıca istatistiksel olaylar tekrarlanabilmektedir. (Emhan 2010: 211)

Belirsizliklerin ve riski kaldırma kapasitesinin zaman içindeki devinimi aşağıdaki şekilde rahatça görülmektedir.



Şekil 1. Risk ve Belirsizlik İlişkisi

Kaynak: Kıral, H.2018:6.

Belirsizlikler, işletmelerde üst yönetimin alacağı kararlar neticesinde aşağıdaki şekilde sınırlandırılabilir:

- Riskin ortaya çıkma olasılığı netleştirilmeye çalışılır ve varsa riski tetikleyen unsurlar tespit edilir.
- Riskin gerçekleşmesi durumda, hangi aksiyonların alınacağına yönelik çalışmalar yürütülür.

Burada dikkat edilmesi gereken noktalardan biri, riskin şu anda mevcut olmaması, ileride gerçekleşme ihtimali olan bir olay olmasıdır. (Bakkal, Kasımoğlu, Tunç 2016:38-39.)

Bu kapsamda detaylı düşünüldüğünde de, her riskin bir fırsat içerdiği gibi, her fırsatın da bir risk içerdiği noktasına kolaylıkla varmak mümkündür.

2.2. Risk Türleri

Risklerin sınıflandırılmasının birçok farklı yöntemi mevcuttur ve işletmeye/işletmenin ait olduğu sektöre göre de farklılıklar gösterebilmektedir.

Alman ekolünde kullanılan ifadeleriyle- gerçek riskler ve spekülatif riskler olarak ikiye ayrılmaktadır. Gerçek riskler sadece gerçekleşme potansiyeli olan tehditleri ifade ederken, spekulatif riskler hem tehdit hem fırsat olarak ortaya çıkabilecek olayları ifade etmektedir. Aşağıdaki tabloda bu ayrımın detaylarını görebiliriz:

Tablo 1. Gerçek ve Spekulatif Risk Ayrımı

Gerçek Riskler	Spekülatif Riskler
Sadece tehditleri ifade eder.	Hem tehdit hem de olası fırsatları ifade eder.
Marka ile ilgili riskler	Yatırımlara yönelik riskler/fırsatlar
Yükümlülüklere ilişkin riskler	Pazar riskleri/fırsatları
Ürün geri çağırma	Döviz kuru riskleri/fırsatları
Üretimdeki teçhizatın zarar görmesi	Personel kaynaklı riskler/fırsatlar
Kısmen sigortalanabilir olan riskler	Sigortalanamayan riskler
DAR ANLAMDA RİSK YÖNETİMİ	
GENİŞ ANLAMDA RİSK YÖNETİMİ	

Kaynak: Hoffmann K. H. 1985:11.

Yukarıda yer alan sınıflandırmaya ek olarak riskler, işletmenin kontrolünde olan riskler ve işletmenin kontrolünde olmayan riskler olarak ikiye ayrılmaktadır. İşletmenin kontrolünde olmayan riskler politik riskler, pazar kaynaklı riskler, ekonomik riskler ve çevresel risklerdir. Bu risklerin yönetimi işletmede olmadığı için azaltılması/yok edilmesi işletmenin elinde de değildir. Bu riskler, içinde bulunulan ülkeye ve

daha küresel bir bakış açısıyla dünyanın içinde bulunduğu siyasal, iktisadi durumlara bağlıdır. İşletmenin kontrolünde olan riskler içinde ise, operasyonel yani faaliyet riskleri ve finansal riskler mevcuttur. Bu risklerin yönetimi; işletme yönetiminin alacağı aksiyonlara, işletmenin stratejilerine ve hedeflerine bağlıdır. (Demir Pali, Adiloğlu 2020:80-81).

Bir başka sınıflandırma yöntemine göre, işletmenin elinde olan/olmayan tüm riskleri dört grupta inceleyebiliriz:

- Stratejik Riskler
- Operasyonel Riskler (Faaliyet Riskleri)
- Çevresel Riskler
- Uygunluk (Mevzuat) Riskleri
- Finansal Riskler

2.2.1. Stratejik Riskler

Önceden öngörülmesi çok kolay olmayan, ekonomik, siyasi, sosyal nedenlerden kaynaklanan ve işletmenin hedeflerine ulaşmasını tehdit altında bırakan risklerdir. Bu riskler, işletme dışı faktörlerden kaynaklanabildiği gibi işletme içi faktörlerden de kaynaklanabilir. İşletmenin içinde olduğu sektöre ait riskler, müşteri portföyü ve rekabet konularına yönelik riskler, mevzuat değişikliklerinden kaynaklanan ve stratejik olarak nitelendirilebilecek riskler dış faktörlerden kaynaklanan risklere örnek olabilir. Aynı şekilde şirketin itibarına yönelik riskler, patent vb. konulardaki riskler de iç faktörlerden kaynaklanan risklerdir. Stratejik risklerin gerçek bir başı ve sonu olmayabilir. Bu nedenle stratejik riskler bir olay olarak değil süreç olarak düşünülerek yönetilmelidir. (Allan & Davis, 2006:10).

Stratejik risk kavramı aynı zamanda stratejik çözümleri de vurgulamaktadır. Bu noktada tüm işletmeler aşağıdaki unsurları dikkate almalıdır. (Pickett, 2005: 12)

- Risk iştahı ile risk stratejisinin uyumlu hale getirilmesi
- Risk cevaplarına yönelik çeşitliliğin artırılması
- Operasyonel kayıpların ve sürprizlerin azaltılması
- Çoklu risklerde entegre risk cevaplarının oluşturulması
- Olası fırsatların fark edilebilmesi için gerekli çalışmaların yapılması

Stratejik riskler, işletmenin tüm stratejisini ve sürdürülebilirliğini etkileme potansiyeli olan riskler olduğu için üst yönetim ve yönetim kurulu, bu riskleri tanımlamalı ve riskleri izlemek için bir yapı oluşturmalıdır. Riskin vereceği hasarın azaltılabilmesi için proaktif bir yaklaşım benimsemelidir. (Frigo, Anderson, 2011:83).

Stratejik riskler içinde en dikkatli yönetilmesi gereken risk grubu, itibar riskleridir. Kurumsal itibar, işletmelerin sahip olduğu önemli bir değerdir. Bir işletmenin tüm paydaşlarının zihninde elde ettiği soyut ve çok önemli bir kıymettir. Bu paydaşlar arasında müşteriler, ortaklar, çalışanlar, tedarikçiler ve aynı pazarda yer alınan rakipler de yer almaktadır. İtibarın elde edilmesi çoğunlukla zor olurken, kaybedilmesi nispeten kolay olabilmektedir. Bu nedenle işletmelerde özellikle kurumsal iletişim veya halkla ilişkiler birimleri bu konuda detaylı çalışmalar yürütmektedirler. İşletmeler, itibar riskini yönetirken tüm paydaşlara zamanında, hızlı, doğru bilgi akışını sağlamayı hedeflemektedirler. (Uzunoğlu, Öksüz, 2013:120)

Bazı stratejik riskler, sürdürülebilirlik konusuyla da ilgili olabilmektedir. İşletmelerin sürdürülebilirlik konusunda uzun dönemli hedefleri olmalıdır. Bu hedeflere doğru giderken işletme yöneticileri proaktif bakış açısıyla neyin doğru gittiğini, neyin gitmediğini tespit edebilecek öngörüye ve deneyime sahip olmalıdırlar. Ancak bu şekilde stratejik risklerin daha az karşılarına çıkmasına katkıda bulunabilirler.

2.2.2. Operasyonel Riskler

İşletmenin faaliyetlerini yerine getirmesi esnasında karşılaşabileceği personel, teknoloji, bilgi-işlem, iş akışı kaynaklı olan ve işletmeyi zarara uğratma ihtimali bulunan tüm iç ve dış olaylar operasyonel risk olarak değerlendirilmelidir.

İnsan kaynağına yönelik riskler içinde; performans riski, eğitimde başarısızlık riski, çalışan devir hızı riski sayılabilmektedir. İşletmelerde yönetim kademesinde yer alan kişilerin, çalışanların bilgi yetersizliğinden, ihmalinden, görevlerini kötüye kullanmalarından ya da kasıtlı olarak suç teşkil edecek olaylara karışmalarından kaynaklanan riskler bu kapsamda değerlendirilmektedir. Personele yönelik risklere neden olan faktörler arasında her seviyedeki çalışanın bilgi/ tecrübe yetersizliği, ücret azlığı, motivasyon eksikliği, üzerindeki aşırı iş yükü, iş yerinde organizasyonel düzenin oturmamış olması (çalışma şartlarındaki sıkıntılar) da yer almaktadır. (Yereli, 2007:19) Son dönemde evden çalışma düzeninin yaygınlaşmasıyla çalışanların mevcut çalışma şartlarıyla sorunlar yaşayabildiği ve sürekli bir iyileştirme beklentisi içinde oldukları gözlemlenmektedir. Bu noktada işveren ile çalışan arasında beklentilerin ve

şartların açıkça görüşülmesi ve netleştirilmesi önem arz etmektedir. Ayrıca yanlış pozisyonlara yanlış kişilerin istihdam edilmesi de insan kaynakları alanında ortaya çıkabilecek riskleri önemli ölçüde artırabilmektedir. Burada işe alım ve terfilerde alanında uzman kişilerden danışmanlık alınabilmekte ya da bu kişiler işletme içinde istihdam edilerek bu risk türüne yönelik önlem alınmış olabilmektedir.

Süreçlere yönelik oluşan risklerde ise; iş akışlarında oluşabilecek riskler, mal tedariği veya satışı esnasında oluşabilecek riskler, müşteri memnuniyetine yönelik riskler örnek olarak verilebilir. Yetersiz ya da içinde problemler barındıran iş süreçlerinden ve sistemlerden kaynaklanabilecek zararlar da operasyonel riskler olarak tanımlanmaktadır.

Bilgi-işlem ve teknoloji alanında da, bilgi-işlem sistemlerinde (donanım veya yazılım kaynaklı) meydana gelebilecek riskler, virüs ve uygun olmayan yazılım kaynaklı riskler yer almaktadır. İşletmelerde bilgi işlem riskleri içinde risklerin en çok meydana geldiği alan muhasebe bilgi sistemleridir. Çünkü bu sistemler, işletmelerin operasyonlarına devam edebilmeleri için olmazsa olmaz teknik alt yapıyı oluşturmaktadır ve işletmelere varlıkların nereden kaynaklandığını, kaynaklarının nerelere harcandığını, tasarruflarının, giderlerinin/gelirlerinin neler olduğunu anlatan teknik çözümlerdir. Bu noktada ilgili sistemlerin her noktasının titizlikle ele alınması gerekir.(Yereli, 2007:16) İş,letmelerin telekomünikasyon sistemlerinden kaynaklanabilecek sıkıntılar, işletmenin en büyük varlığı olarak sayabileceğimiz verilerde olabilecek kayıplar sistemlerin/sistem modellemelerinin en başında hatalı tasarlanması sonucu oluşabilecek problemler, veri güvenliği konusunda karşılaşılabilecek sorunlar bu kapsamda değerlendirilmesi gereken riskler arasında yer almaktadır. Her risk çeşidinde olduğu gibi bilgi işlem ile ilgili risklerde de insani hatalar her zaman mevcut olabilir. Kişisel hataların azaltılmasına yönelik sistemin her alanına gerekli kontrollerin konulması da bu sebeple çok önemlidir. Çalışanların günlük operasyonlarında çalıştıkları sistemlerde oluşacak olan risklerde; çalışanlar, işletmedeki süreçler, prosedürler gibi riskin kaynaklanabileceği noktalara eğilmek yerine işletmeler genelde donanım, yazılım gibi maddi ve maddi olmayan varlıklardaki güvenlik açıklarına odaklanmaktadırlar. (Spears ve Barki, 2010 :503). Zamanla teknolojinin çok hızlı gelişmesinin etkisiyle, işletmelerde kullanılan bilgi işlem sistemleri çok gelişmiş ve çeşitlenmiştir. Bu sebeple, geçmiş ile kıyaslandığında işletmede kullanılan sistemlerin çokluğu ve karmaşıklığı ile doğru orantılı olarak oldukça fazla miktarda riskle de karşı karşıya kalındığı gözlemlenmektedir.

2.2.3. Çevresel Riskler

İşletme ile herhangi bir bağlantısı olmayan, tamamen dış etkenler neticesinde ortaya çıkan bazı riskler bu kapsamda değerlendirilebilmektedir. Dış kaynaklı operasyonel risklere dışarıdan alınan hizmetlerde aksaklık yaşanması ya da yangın, deprem, sel gibi olağanüstü olaylar örnek olarak verilebilir. Dünya Ekonomik Forumu, her yıl olduğu gibi 2024 yılında da Küresel Riskler Raporu'nu yayınlamıştır. Bu rapora göre, yapılan anket çalışmaları sonucunda, katılımcıların % 54'ünün ilerleyen dönemde, olağanüstü risklerin artış eğiliminde olacağını öngördüğü ileri sürülmüştür. Rapor sonuçları incelendiğinde, olağan dışı hava olayları, doğal felaketler, iklim değişiklikleri, terör saldırıları, yaşam maliyetlerinin artması, siber saldırılar, bilgi kirliliği gibi risklerin tüm dünyanın geleceğini tehdit edeceği tahmin edilmektedir. (The Global Risks Report, 2024).

Çevresel riskler konusunda, insanların farkındalığının artırılmasına yönelik çabalar günümüzde bu riskleri sıkça konuşulan bir konu haline getirmiştir. Küresel salgınlar, çeşitli hastalıklar (özellikle bulaşıcılığı yüksek olan viral hastalıklar), terör saldırıları, depremler, heyelanlar, iklim krizi gibi felaketler yüzünden insanoğlu artık pek güvende değildir ve maalesef ki kendini de güvende hissetmemektedir. (Tekin, S. 2020). Önceden öngörülemeyecek olan bu olağanüstü olaylara karşı işletmelerin kendilerini mümkün mertebe güvence altına almalarını sağlayabilecek önlem planlarını yapmış olmaları, sigorta vb. işlemleri doğru bir şekilde yürütüyor olmaları gerekmektedir. (Özbilgin, G. 2012: 89) Ayrıca gelişen teknolojinin bize verdiği bilgi işlem alt yapıları ve çeşitli olanaklar sayesinde gerçek zamanlı verilerin kullanılması ve afet kaynaklı risklere yönelik tam zamanlı ve doğru tahminlerin yapılması, olası bir afet sonrasında oluşabilecek hasarların önlenmesi ve doğru zamanda doğru yere doğru şekilde müdahale edilmesi sonucu doğuracaktır, Bu nedenle teknolojik gelişmelerden bu konuda faydalanmak büyük önem arz etmektedir. (Coşandal, Partigöç 2022:158).

2.2.4. Uygunluk Riskleri

İşletmeler faaliyetlerini ve tüm tüm paydaşlarıyla olan ilişkilerini kendilerini çevreleyen ulusal ve uluslararası bir dizi yasal düzenlemelere - *ticari, yasalar, medeni kanun, dış ticaret-gümrük ve vergi kanunları, sermaye ve para piyasası mevzuatı, sigorta kanunları, çevre kanunları, insan hakları, karaparanın aklanması, sektörel düzenlemeler, lisanslar, sözleşmeler, bunlarla bağlantılı uluslararası anlaşmalar vb gibi* - uygun şekilde gerçekleştirmek zorundadır. İşletmeler için en büyük risk türlerinden

biri de bütün bu yasa ve düzenlemelere uygunluk/uyum riskidir. Yasalara uymayan faaliyetler ve işlemler dolayısıyla işletmeler maddi cezai yaptırımlarla karşı karşıya kalabilecekleri gibi faaliyetlerinin durdurulması veya itibarların zedelenmesi gibi büyük zararlar doğurabilecek pek çok olumsuz sonuçlarla karşılaşabilirler.

2.2.5. Finansal Riskler

Finansal riskler, istenmeyen finansal sonuç veya etkiye sahip olay veya sonuçlardır. Finansmanın korunması ve kayıpların önlenmesi ile ilgili olan bu riskler (Lancaster, Goff, 2023); gelir kaybı riski, daha yüksek veya beklenmedik harcama riski, varlıklara/yatırımlara ilişkin riskler, borç veya kredi finansmanı ve likiditeyle ilgili riskler, raporlama riskleri ve işletmedeki yönetsel karar ve eylemler de dahil iş ve işlemlerden kaynaklanan ve finansal sonuç doğuran bütün riskler ile piyasa ve kur/kambiyo riskleri bu tür risklere örnek verilebilir.

Esasen finansal risk, işletmenin bir iş yatırımı veya sermaye kaybı da dahil olmak üzere başka bir kararda para kaybetme olasılığıdır. Genel olarak bu risk türü, kendi içinde; operasyonel risk, kredi riski, piyasa riski, likidite riski, yasal risk ve döviz kuru riski dahil olmak üzere finansal alana giren altı risk türü şeklinde gruplandırılabilir.

Kuruluşlar bu risk türlerini anlayarak ve inceleyerek finansal araçlar, portföy yönetimi, bütçeleme ve tahsis ve varlık yönetimi konularında en iyi uygulamaları benimseyebilirler ve daha iyi finansal karar alma süreçleri oluşturabilirler.

Finansal risk yönetimi bağlamında operasyonel risk işletmenin karını etkileyebilecek günlük işlemlerde öngörülemeyen olayları kapsar. Örneğin, bir üretim tesisinin veya veri merkezinin birkaç saat boyunca devre dışı kalması, işletme için gelir kaybına neden olabilir. Bu tür riskler, sistemler, süreçler, kişiler veya dış olaylar günlük işlevlere müdahale ettiğinde gerçekleşir. Operasyonel riski tamamen ortadan kaldırmak zordur; çünkü süreçler, kişiler ve sistemler olduğu sürece hatalar olacaktır. Ancak, operasyonel riski kabul edilebilir bir risk toleransı eşiğiyle sınırlamak için azaltma stratejileri uygulayarak, şirketler herhangi bir kalıntı riske rağmen gelişmeye devam edebilir. Finansal risk yönetimi (FRY) ve operasyonel risk yönetimi (ORY) ekipleri, artan etkililik için potansiyel riskleri ele almak ve yönetmek üzere iş birliği yapabilir.

Kredi riski, bir müşterinin veya borçlunun ödemeler gibi finansal yükümlülüklerini yerine getirememesi riskidir. Şirketler, sigorta ve teminat yoluyla kredi riskini azaltmak için adımlar atabilir, ancak bazı taraflar yine de temerrüde düşebilir. İşletmeler, geçmişteki kredi temerrüt örneklerini anlamalı ve kıyaslamalı, eğilimleri analiz etmeli ve yüksek riskli işlemleri işaretlemek veya düşük kredi notuna sahip alıcıların kredi almasını önlemek gibi gelecekteki kredi risklerini yönetmek için buna göre hareket etmelidir. Kredi kontrolleri, bir müşterinin veya borçlunun ertelenmiş ödemeler için uygunluğunu değerlendirmek için kullanılan bir diğer yaygın araçtır.

Piyasa riskleri, belirli bir sektördeki risk veya makroekonomik koşullar üzerindeki jeopolitik etkiler gibi sermaye piyasaları ve finansal piyasalarla bir bütün olarak ilgilidir. Piyasadaki yüksek faiz oranları, insanları kredi almaktan caydırır ve tasarrufları teşvik eder, bu da borç verenler ve bankaların gelirleri için potansiyel bir risk oluşturur. Sermayenin mevcudiyeti şirketlerin değerlemelerini etkileyebilir. Piyasa risklerini tahmin etmek zordur ve aniden ortaya çıkabilir, ancak güçlü bir FRY programını sürdürmek kuruluşun uyanık ve hazırlıklı olmasını sağlayabilir.

Likidite riski, bir kuruluşun nakit veya fon eksikliği nedeniyle finansal yükümlülüklerini yerine getirememesi veya ödeme yapamaması durumunda kredi riskinin tersine benzer. Likidite riski, bir işletme için varoluşsal bir tehdit olabilir ve hatta devam eden bir işletme riskine yol açabilir. Nakit akışını, yükümlülükleri ve varlıkları dengeli bir şekilde yönetmek ve düzenli FRY uygulamaları ve kontrolleri sürdürmek, kuruluşların likidite riskini sınırlamasına ve şirketin nakit akışını sağlıklı tutmasına yardımcı olabilir.

Yasal/ veya uyumluluk riskleri, daha önce de açıkladığımız gibi işletme ve sektör için gerekli olan yasal, düzenleyici veya uyumluluk gerekliliklerini karşılayamamaktan kaynaklanan bir kayıpla ilişkili risklerdir. Yasal riskler, kusurlu bir ürünün bedensel yaralanmaya neden olması gibi davalar nedeniyle oluşan finansal kayıp riskini içerebilirken, uyumsuzluk riski para cezalarına ve satış kayıplarına yol açabilir. FRY'yi kuruluşun daha büyük kurumsal risk yönetimi (veya eşdeğeri) işleviyle entegre etmek, risklerin silolar arasındaki çatlaklardan sızmamasını sağlar ve risk yönetiminde iş birlikçi ve proaktif bir yaklaşımı teşvik eder.

Döviz veya kur riskleri, döviz kurunda oluşan beklenmeyen değişikliklerin işletmenin finansal durumunu etkilemesi durumunda gerçekleşir. Döviz kurlarındaki dalgalanmalar, özellikle ani ve öngörülemeyen

olduklarında, bir işletmenin yatırımlarının, finansal durumunun ve varlıklarının değerlemesi üzerinde önemli bir etkiye sahip olabilir. Bu tür risklerin çok uluslu şirketlerde; ithalat ve ihracata yoğun yatırım yapan şirketlerde; ve yabancı ülkelerde önemli finansal varlıklara sahip işletmelerde ortaya çıkma olasılığı daha yüksektir. Bu ekonomik maruziyeti yönetmek, tesislerin konumlarını çeşitlendirmek; ürünlerin satıldığı pazarlar; ve malzeme kaynakları gibi operasyonel stratejiler yoluyla sağlanabilir. Şirketlerin döviz kuru değişikliklerinin etkisini sınırlamalarına olanak tanıyan döviz akışları ve döviz takasları gibi döviz riskiyle ilgili özel azaltma seçenekleri de mevcuttur.

2.3. Risk Yönetimi Kavramı

Risk yönetimi kavramı ilk olarak bankacılık ve sigortacılık alanında yani finans sektöründe ortaya çıkmıştır. Daha sonra bu kavram diğer sektörler tarafından da kabul görmüş ve ancak birkaç yüzyıllık dönem içinde detayları oluşturulmuştur. Risk yönetimi kavramının gelişmesinde, II. Dünya Savaşı'ndan sonra globalde yaşanan gelişmeler çok etkili olmuştur. Teknolojinin kullanımının artması, iş süreçlerinin karmaşıklaşması, ulusal ve uluslararası rekabetin artması bu gelişmelerden en önemlileridir.

Amerika Birleşik Devletleri'nde risk yönetimi terimi ilk kez 1950'lerin sonlarında kullanılmıştır. Risk yönetimi, gerçekleşme potansiyeli olan tüm olasılıkların planlaması şeklinde de ifade edilebilir. "Eğer olursa ne olur?" ve "ya olursa" sorularının cevaplanması da risk yönetimini doğurmuştur denilmektedir. (Emhan 2010, 213)

Son yıllara gelindiğinde de özellikle 2008-2009 yıllarında yaşanan global krizin işletmeler üzerindeki etkisinin büyüklüğünde en önemli faktörlerden birinin işletmelerin etkili bir kurumsal risk yönetimi sisteminin olmaması, bu sisteme sahip olanların da sistemi verimli şekilde kullanmamaları olduğu tüm kaynaklarda sıklıkla belirtilmektedir. Bu noktada tabii ki iç kontrol ve iç denetim sistemlerinin işletmelerde ne şekilde uygulandığı ve uygulamada mevcut olan eksiklikler de dikkatlice irdelenmelidir.

Risk yönetimi, risklerin zamanında ve doğru bir şekilde tanımlanması, sayısal olarak ifade edilebilecek hale getirilmesi yani ölçümlenmesi, düzenli olarak takip edilmesi, bu riskleri minimize edecek veya ortadan kaldıracak önlem planlarının yapılması ve sonuçların ilgililere raporlanması gibi süreçleri kapsamaktadır. Burada diğer bir önemli konu ise, riskin vereceği zarar hesaplanırken aynı zamanda da riskin gerçekleşme olasılığı da ortaya konulmalıdır. Ancak riskin gerçekleşme olasılığı ile gerçekleştiğinde yaratacağı hasarın birbirine bağlı olmadığı akıldan çıkarılmamalıdır. Örneğin deprem, sel gibi doğal afet kaynaklı risklerin

gerçekleşme ihtimali düşük olmasına rağmen, gerçekleştiğinde yaratacağı hasar oldukça büyüktür. Gerçekleşme olasılığı birçok işletmede yüzde ile (%1-%100) ifade edilmektedir.

Risk ile karşı karşıya kalmayacak bir işletmenin var olması mümkün değildir. Bu nedenle etkili risk yönetimi uygulamalarını hayata geçirmek ve titizlikle önlem planlarını oluşturmak işletmenin geleceğinin garanti altına alınmasında önemli rol oynamaktadır.

Risk yönetimi uygulamaları şirketler arasında farklılık gösterebilir. Şirketlerin ait olduğu sektörler, büyüklükleri, ulusal veya uluslararası olmaları gibi birçok faktör burada çok etkilidir.

Riskin tanımlanması, değerlendirilmesi, yönetilmesi konusunda geleneksel bakış açısı ile modern bakış açısı arasında önemli farklılıklar vardır. Bu farklılıklar aşağıdaki tabloda detaylı bir şekilde ifade edilmiştir.

Tablo 2. Risk Kavramına Geleneksel ve Modern Bakış

Riske Geleneksel Bakış	**Riske Günümüzdeki Bakış**
Risk, kontrol altında tutulması gereken olumsuz bir durumdur.	Risk aynı zamanda bir fırsattır.
Risk, işletme içerisinde birimler tarafından yönetilir.	İşletme çapında bir bütün olarak yönetilir.
Risk ölçümü subjektiftir.	Risk ölçümü objektiftir.
Risk yönetiminin sorumluluğu, fonksiyonel birimlerin yönetimindedir.	Risk yönetimi, üst yönetim ve fonksiyonel birimlerin yönetimi tarafından beraber yürütülür.
Yönetim Kurulu'nun iç kontrolü sağlayan bir iç denetim departmanı bulunur.	Yönetim Kurulu'nun, etkili risk yönetimi için risk komitesi vardır.

/Kaynak: Açıkalın 2012:3

Bu noktada, bakış açılarına da değindikten sonra, doğal risk ve artık risk kavramlarından da bahsetmek gerekmektedir. Doğal risk, herhangi bir sürecin doğasında olan ve bu riskin ortadan kaldırılması için önlem alınmayan durumlarda ortaya çıkan risktir. Alınan önlemlere rağmen olayın gerçekleşmesi halinde oluşan risk ise artık risk olarak ifade edilebilir. Örneğin, erozyona müsait dere yatağı gibi bir alana kurulan fabrikada sel sebebiyle oluşabilecek ve önlem alınmaması halinde karşılaşabileceğimiz riskler doğal risktir.

Bu örnekteki fabrikaya önlem maksatlı sigorta yapıldı ise, risk gerçekleştiğinde zararın büyük kısmı sigorta tarafından karşılanmaktadır. Geriye kalan kısım ise artık risk olarak değerlendirilmektedir. (Özbek 2012:238)

Finansal kontrol konusu ile risk yönetimi konusunun oldukça fazla ortak noktası vardır. Bunlardan en önemlisi ise başarıya odaklanmalarıdır. Günümüzde başarının daha geniş anlamda anlaşılması gerekmektedir. Başarının en yüksek ölçüsü, her zaman şirketin değerinin artmasıdır. Bu başarı ölçüsünden değer artışıyla bağlantılı diğer değişkenler de elde edilebilmektedir. Alman ekolünde risk yönetimi kavramı genellikle finansal kontrol ve planlama alanı içinde değerlendirilmektedir. (Finke, R., 2005;23-24)

Risk konusuna giriş yapılırken değinilmesi gereken iki önemli kavram da risk iştahı ve risk toleransıdır. Risk iştahı, bir işletmenin hedefleri, misyonu, vizyonu ile doğru orantılı olarak kabul edebileceği en kapsamlı risk düzeyini ifade etmektedir. Diğer bir ifadeyle, işletme yönetiminin önlem planı yapmadan önce alabileceğini düşündüğü risk oranıdır. (Bozkurt, 2010:19)

Risk iştahının belirlenmesine yönelik COSO'da da yer alan adımlar aşağıda yer almaktadır:

1. İşletme öncelikle karşılaştığı tüm risklerin mevcut seviyesini, işletmenin üzerine alabileceği en yüksek risk düzeyini, olası riskleri ve risklerin sonuçlarına yönelik alması gereken tutumları dikkate almalıdır.
2. İşletme için uıygun olan risk iştahı belirlendikten sonra, belirlenen risk iştahına yönelik hemen işletmenin her seviyedeki çalışanına bilgi verilmelidir.
3. İşletmede gerçekleşme ihtimali olan tüm riskler, değerlendirme aşamasında nicel ve nitel ölçütlere göre analiz edilmeli ve devamlı izlemeye tabi tutulmalıdır. (Olson ve Wu, 2015: 6)

Risk iştahı, genel olarak belirlenebileceği gibi, şirketin belli alanları için farklı olarakta belirlenebilmektedir. Örneğin, yasal/mevzuat konularında oluşabilecek riskler çok ciddi maddi kayıplara sebep olabileceği için bu alanda risk iştahı düşük belirlenebilir, araştırma-geliştirme/üretim/satış gibi konularda ise riskler ve fırsatlar beraber değerlendirilebileceği için şirketler risk almaya daha hevesli olabilmektedir. Bu durumda da risk iştahı göreceli olarak daha yüksek belirlenebilmektedir. Değerlendirme yapılırken işletmenin büyüklüğü, bulunduğu sektör, sermaye yapısı vb. birçok konu titizlikle dikkate alınmalıdır. Risk iştahı yükseldikçe hem olası zarar hem de aynı zamanda olası gelir yükselebilmektedir.

Etkili risk yönetimi ortamında önemli olan işletme için stratejik anlamda doğru kararların alınabilmesidir. (Bakkal, Tunç, Kasımoğlu, 2016:44-45)

Risk toleransı ise, işletmenin hedeflerine ulaşma yolunda karşılaşabileceği risklere yönelik olarak kabul edilebilir durumda olan sapma derecesini yani değişkenliği ifade eder. Aynı zamanda risk toleransı bize işletmenin esneklik payı hakkında da önemli bilgi vermektedir. Risk iştahı ve risk toleransı birbirine yakın kavramlardır, ancak risk iştahı çok daha geniş bir ifadedir. (Bozkurt, 2010:20) Risk iştahı, işletmenin ek bir tane bile risk almamasına yönelik sınırlar koymaktadır. Risk toleransı ise bu noktada daha faaliyete özel ve dar kapsamlı kalmaktadır. (Bakkal, Tunç, Kasımoğlu, 2016:46)

Aşağıda risk iştahı ve risk toleransına yönelik iki ifade görülmektedir. Bu iki cümle arasındaki farklar birinin stratejilere yönelik ve genel olması, diğerinin ise çok daha spesifik ve aksiyona yönelik olmasıdır.

Risk İştahı ->" Hasta güvenliği birinci önceliğimizdir. Tüm hastaların ihtiyaçlarına anında yanıt verme düzeyi ile bu hizmeti vermenin maliyeti arasında bir dengeleme yapmak zorunda olduğumuzun da farkındayız."

Risk Toleransı->"Personel kadromuzu, standart hastalara randevu saatinden itibaren 15 dakika içinde, acil hastalara ise 5 dakika içinde müdahale edilebilecek şekilde planlıyoruz. Ama yönetim, nadir durumlarda ve yaşamı tehdit etmeyen hallerde bu hizmetin 4 saat içinde verilmesini de kabul etmektedir." (Carmichael, M.,2022)

Bu noktada değinilmesi gereken diğer bir kavram risk kapasitesidir. Bu kavram, işletmenin dayanabileceği maksimum zorluğu, sıkıntıyı gösterir. Risk kapasitesi, işletmenin elindeki nakit veya nakit olmayan kaynaklar, alabileceği krediler ile de ölçülebilmektedir. (Bozkurt, 2010:19) Risk kapasitesinin belirlenmesinde bilançonun detalı analiz edilmesi, alacakların ve borçların incelenmesi mantıklı bir yaklaşım olabilmektedir.(Cordell, D.M.,2002:30)

2.4. Risk Yönetiminin Amacı ve Tarihçesi

Risk yönetiminin amacı, işletmenin karının en üst seviyeye çıkarılmasını sağlamak ve aynı zamanda işletmenin sürdürülebilirliğini güvence altına almak şeklinde tanımlanmaktadır. Risk yönetimi süreci, amacına ulaşabilmek için gerekli tüm adımların atılmasını, kararların alınmasını da içine almaktadır. (Emhan 2010: 213)

Risk yönetiminin temel hedefi, gelecekte işletmeye zarar verme ihtimali olan olayları ve bu olaylar neticesinde ortaya çıkacak olan olumsuz neticeleri azaltmak ve sonuçta işletmenin hedeflerine ulaşmasını sağlamaktır. Bir işletmede risk yönetimi süreci iyi kurgulanmış ise, işletmede mevcut olan tehditlerin minimize edilmesi, fırsatların da etkili şekilde yönetilmesi mümkün olmaktadır. Risk yönetimi bu noktada, işletmenin stratejilerini desteklemeli, işletme ile ilgili tüm paydaşları koruyup gözetmeli ve işletmeye değer katmalıdır. (Bakkal, Tunç, Kasımoğlu, 2016:52)

Risk yönetimi kavramı, yukarı da değinildiği üzere ilk olarak 1950'lerde sigorta şirketlerinde ortaya çıkmış, 1970'lerden itibaren de diğer sektörlerde de kullanılmaya başlanmıştır. Ancak tabii ki 1999'dan başlayarak meydana gelen ve temelinde çeşitli muhasebe, finans, raporlama hilelerinin yer aldığı başta ENRON XEROX, Worldcom, Adelpha, Tyco, Globalcrossing olmak üzere birçok şirketin iflas etmesi üzerine risk yönetimi konusu büyük önem kazanmış ve çeşitli yasal düzenlemelerin yapılmasını zorunlu kılmıştır. Yaşanan skandallar hem şirketlere ve yöneticilerine hem de yıllardır o şirketlerin denetimini üstlenmiş olan denetçilere ve mevcut mevzuata olan güveni bir hayli sarsmıştır. Bu gelişme neticesinde hem ABD'de hem de AB ülkelerinde çeşitli düzenlemeler ortaya çıkmıştır. Bu yasal düzenlemeler aşağıdaki bölümde detaylı anlatılacaktır.

Risk yönetiminin zaman içindeki kat ettiği yol incelendiğinde, üç önemli konunun var olduğu görülmektedir. Bu konuların birincisi, işletmelerin risk yönetiminin kıymetli bir yönetim konusu olduğunu anlamalarıdır. Bu noktada işletmenin kar amacının olması ya da olmaması birşeyi değiştirmemektedir. İkinci konu; işletmenin stratejilerine ve hedeflerine yönelik çalışmalara ağırlık verilmesidir. Üçüncü ve son noktada ise, işletmelerin yavaş yavaş artık kurum bünyesinde entegre bir risk yönetimi sisteminin gerekliliğini anlamaları şeklinde ifade edilmektedir. (Bakkal, Tunç, Kasımoğlu, 2016:52)

Risk yönetiminin nihai amacı; işletmenin geleceğini tehdit eden tüm olaylara karşı aksiyon alabilmek, işletmenin hedeflerine ulaşmasını ve sürdürülebilir şekilde büyümesini sağlayabilmektir. Etkili bir kurumsal risk yönetimi, işletmenin risklerini yönetebilmesi, fırsatlarını da fark ederek işletmeye fayda sağlayabilmesini getirmektedir. Risk yönetimi, işletmeye ve aynı zamanda işletmenin tüm paydaşlarına değer katmayı da amaçlamaktadır. Burada işletmenin kaynaklarının verimli kullanılmasına, işletmenin itibarının korunmasına da dikkat edilmelidir. (Yılancı, 2006:28)

2.5. Risk Yönetimi İle İlgili Yasal Düzenlemeler

Risk yönetimine yönelik hem dünyada hem de ülkemizde birçok düzenleme yapılmıştır. Bunlardan en önemlilerini aşağıda incelenecektir.

2.5.1. ABD'deki ve Avrupa'daki Düzenlemeler

2001 yılı Aralık ayında iflas etmesinden önce Amerika'nın en hızlı büyüyen şirketlerinden biri olarak kabul edilen ve Fortune 500 listesinde beşinci sıraya yerleşmeyi başaran Enron Şirketinin iflasıyla dünya tarihinin en önemli muhasebe skandallarından biri ortaya çıkmıştır. Enron'un finansal kayıtlarında yaptığı manipülasyonlar ile bunları herkesten gizlemesi ve yaşananların bir iflas skandalıyla ortaya çıkması tüm dünyada kurumsal yönetime olan güveni sarsmıştır. Buna benzer durumların tekrar yaşanmaması için ABD'de 2002'de Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Kanunu veya diğer adıyla Sarbanes-Oxley Kanunu (SOX) kabul edilmiştir. Bu kanunun yürürlüğe girmesi ile kurumsal yönetim ve finansal raporlama ilkeleri Amerika Birleşik Devletleri'ndeki borsalarda işlem gören halka açık şirketlerin hepsini kapsayacak şekilde yasal bir zorunluluk haline gelmiştir. Kanunun 302 ve 404. maddeleri çerçevesince şirketlerin finansal raporlamaları üzerindeki risklerin belirlenmesi, belirlenen risklere ilişkin kontrollerin belgelendirilmesi ve değerlendirilmesi zorunlu tutulmuş ve kontrollerin etkililiğinden şirket yöneticileri doğrudan sorumlu tutulmuştur. (Özbek, 2012:208-212)

ABD'de risk yönetimine yönelik düzenlemelerin oluşmasına ve iç kontrol sistemlerinin geliştirilmesine yol açan en büyük faktörler arasında hissedarların güvenlerini sarsan hileli finansal raporlama örneklerinin ve çeşitli konularda ortaya çıkan muhasebe skandallarının yer almaktadır. Aynı durum AB ülkelerinde de ortaya çıkmış ve orada da çeşitli düzenlemeler getirilmiştir. Yalnız ABD'de düzenlemeler daha çok iç kontrol temeli üzerine inşa edilmiş ancak AB ülkelerinde daha geniş kapsamlı ve şirketin tüm süreçlerine yayılan düzenlemeler oluşturulmuştur. Buna ek olarak, oluşturulan yapı ABD'ye nazaran daha esnek ve şirketin kendi özelliklerine göre düzenleme yapmasına imkan verecek şekilde organize edilmiştir. (Van Der Erst, C., Van D.,2009: 25-27).

Kanunlarda bahsedilen iç kontrol ve risk yönetimine ilişkin olarak getirilen yükümlülüklerin hangi yöntem ve yaklaşımlarla hayata geçirileceği konusu, daha sonra COSO tarafından açıklığa kavuşturulmuştur. Bu amaçla 1992 yılında yayımlanan İç Kontrol Çerçevesinin ardından COSO, bu kez 2004 yılında Kurumsal Risk Yönetimi Çerçevesini yayınlamıştır. Sarbanes-Oxley Kanunu ile yatırımcıları ve daha geniş anlamıyla

halkı korumak, daha doğru bilgilendirmek, halka açık şirketlerin denetim standartlarını belirlemek ve denetçilerini denetlemek amacıyla Halka Açık Şirketler Kamu Muhasebe Gözetim Kurulu (the Public Company Accounting Oversight Board-PCAOB) kurulmuştur. Bu Kurul yayımladığı 2 numaralı standartta COSO Çerçevesinin yönetimin değerlendirilmesi için uygun ve elverişli bir çerçeve sunduğunu belirterek, bir anlamda COSO Çerçevesini Amerika'da faaliyet gösteren şirketler için geçerli kılmıştır. (Özbek, 2012:262-263) COSO 2017 yılında kurumsal risk yönetimine yönelik çerçevesini güncellemiştir. Bu güncellemeye yönelik bilgiler aşağıdaki ilgili bölümde verilecektir.

Ayrıca COSO, Uluslararası İç Denetçiler Enstitüsü (IIA), Amerika Yeminli Muhasebeciler Enstitüsü (AICPA), Amerika Muhasebeciler Birliği (AAA), Yönetim Muhasebecileri Enstitüsü (IMA) ve Finans Yöneticileri Derneği'nin (FEI) destekleriyle kurulmuş olan bir yapıdır. Özellikle denetim, muhasebe ve finans alanında faaliyet gösteren önemli mesleki kuruluşların desteği COSO'nun kurumsal risk yönetimi yarışına önde başlamasını sağlamıştır. Ancak, denetim, muhasebe ve finans ağırlıklı bu yaklaşım aynı zamanda, COSO Çerçevesinin kontrol ve uyum temelli olması da sebebiyle yönetim süreçlerine entegre edilmesinde ve stratejik düzeyde uygulanmasında birtakım zorlukları barındırdığını düşündürtmektedir.

COSO çerçevesinin dışında ISO (Uluslararası Standartlar Örgütü), ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği), RIMS (Risk Yönetimi Topluluğu) gibi kuruluşlar da risk yönetimi üzerine rehber veya standartlar yayımlamışlardır. Bu rehberlerden en çok bilineni ISO 31000 dir. ISO 31000, 2009 yılında kurumsal risk yönetimi prensiplerinin uygulamasına yönelik uluslararası mecrada kabul görmüş bir standart olarak yayınlanmıştır. COSO'yu hazırlayan ekibin içinde genellikle denetçiler, muhasebeciler, finans uzmanlar yer alırken, ISO büyük çoğunlukla kurumsal risk yönetimi uygulayıcıları tarafından oluşturulmuştur. Bu standart, işletmelerin pek çok faaliyetinin riskli durumlara sebep olabileceği ve bu nedenle karşı karşıya kalınabilecek risklerin tanımlanıp değerlendirilmesine olanak sağlamaktadır. Riskin derecelendirmesini yaparak, riskin değiştirilip değiştirilemeyeceğini değerlendirerek yönetmektedir. Bu süreç boyunca işletmeler operasyonel faaliyetlerindeki tüm farklılıkları kontrol eder, paydaşlarıyla bunları paylaşır, gerektiğinde onlara danışır ve riskin ele alınması için ek hususların olup olmadığından emin olurlar. (Karaman, Tosuner 2020: 108)

ISO 31000'e göre, etkili bir risk yönetiminin ilkeleri arasında değer yaratmak ve korumak, risk yönetiminin tüm örgütsel süreçlerin ayrılmaz bir parçası olması, üst yönetimin karar destek süreçleri içinde yer alması, sistemli, şeffaf bir süreç olması, her an güncellenmeye müsait olması sayılmaktadır. (Çeliktaş 2018: 486)

Hollanda'da bu konuda düzenlemeler 2008 yılında yayınlanan Hollanda Kurumsal Yönetim Prensipleri içinde yer almaktadır. Risk yönetimini kanunlarına dahil eden ilk ülke ise Almanya'dır. KonTrag (German Law on Corporate Controlling and Transparency) ismi ile bilinen kanunda şirketlerde iç-dış tüm risklerin tespit edilip yönetilebilmesi için risk yönetimi sürecinin kurulmasının gerekliliği anlatılmaktadır.

İngiltere'de ise yasal bir dayanağı olmamasına rağmen 1999'da yayınlanan Turnbull Report, risk yönetimi konusunda başvurulan önemli kaynaklardandır. Bu raporun 2005 yılında yayınlanan güncel versiyonunda "iç kontrol sisteminin, işletmenin hedeflerinin gerçekleştirilmesi açısından önem taşıyan risklerin yönetilmesi açısından kilit bir role sahip olduğu" ifade edilmektedir. "Yönetim Kurulu'nun, işletmeni kendi risklerinin onayladığı haliyle yönetilecek biçimde iç kontrol sisteminin etkili olmasını sağlaması gerektiği, güçlü bir iç kontrol sisteminin var olup olmadığının değerlendirilmesinde ise, işletmenin karşı karşıya kalabileceği risklerin boyutu ve doğasının göz önünde bulundurulması gerektiği" açıklamıştır. (Internal Control – Revised Guidance for Directors on the Combined Code, Financial Reporting Council 2005) 2010 senesinde İngiltere Kurumsal Yönetim Prensiplerinde değişiklik yapılmış ve bu değişiklikte yönetim Kurulu şirketin stratejik hedeflerini gerçekleştirirken almaya hevesli olduğu önemli risklerin menşeiini ve içeriğini belirlemekle yükümlü olduğunu ve yine etkili bir iç kontrol ve risk yönetimi süreci hakkında genel kurula rapor verilmesi gerektiğini belirtilmiştir. (Özbek 2012:247)

2004 yılında AB'de de yayınlanan Şeffaflık Direktifi'ne göre (Transparency Directive), bir AB ülkesinde faaliyet gösteren şirketlerin faaliyet raporlarının işletmenin önümüzdeki altı ayda karşılaşması olası olan risklerine yönelik bilgi içermesi gerektiği açıkça ifade edilmiştir. Yine aynı doğrultudaki bir gelişme de 2006 yılında 8.Direktif içinde bir düzenleme yapılmış ve halka açık şirketlerin mali raporlama süreçlerini, iç kontrol, iç denetim ve risk yönetimi sistemlerinin doğru çalışıp çalışmadığını denetlemek üzere denetim komitesi kurması zorunlu hale getirilmiştir. (Van Der Erst, C., Van D.,2009: 29).

Dünya'nın çeşitli ülkelerinde COSO ve ISO 31000 gibi uluslararası standartları/çerçeveleri baz alarak çeşitli başka çerçeve ve rehberler yayınlanmıştır. Bunlar arasında Avustralya ve Yeni Zelanda risk yönetim modeli olan AS/NZS 4360 Risk Yönetim Rehberi ve İngiltere'nin BS31000 Risk Yönetim Rehberi de yer almaktadır. (Kıral 2018:8).

2.5.2. Türkiye'deki Yasal Düzenlemeler

2.5.2. 1. TTK (Türk Ticaret Kanunu)

Küreselleşmenin etkisiyle işletmeler arasında rekabet de artmış, yoğun rekabet ortamında varlığını sürdürmek isteyen işletmelerin ortaya çıkabilecek riskleri öngörme kabiliyetine sahip olmaları ve aynı zamanda da meydana gelebilecek fırsatları da fark edip ona göre aksiyon planları hazırlamaları ihtiyacı doğmuştur. Geleneksel risk yönetiminden kurumsal risk yönetimine geçişin en büyük kazanımı sürece fırsat yönetiminin dahil olmuş olmasıdır. İşletmelerde layıkıyla kurumsal risk yönetimi uygulayabilmek için buna yönelik komiteler kurulmaktadır. Türkiye'de 2012 yılında yürürlüğe giren (Yeni) Türk Ticaret Kanunu'na göre, halka açık işletmelerde riskin erken saptanabilmesi, yönetilebilmesi için uzman bir ekibin varlığı ve bu konuda detaylı çalışmaların yapılması gerekli hale gelmiştir. (Gacar 2017:123).

Türk Ticaret Kanunu'nun 378 nolu "Riskin Erken Saptanması ve Yönetilmesi" adlı maddesinde konuyla ilgili aşağıdaki hüküme yer verilmiştir:

"(1) Pay senetleri borsada işlem göre şirketlerde, yönetim kurulu, şirketin varlığını, gelişmesini ve devamını tehlikeye düşüren sebeplerin erken teşhisi, bunun için gerekli önlemler ile çarelerin uygulanması ve riskin yönetilmesi amacıyla, uzman bir komite kurmak, sistemi çalıştırmak ve geliştirmekle yükümlüdür. Diğer şirketlerde bu komite denetçinin gerekli görüp bunu yönetim kuruluna yazılı olarak bildirmesi halinde derhal kurulur ve ilk raporunun kurulmasını izleyen bir ayın sonunda verir."

"(2) Komite yönetim kuruluna her iki ayda bir vereceği raporda durumu değerlendirir, varsa tehlikelere işaret eder, çareleri gösterir. Rapor denetçiye de yollanır."

Söz konusu madde hükmü, şirketlerin risk yönetimine yönelik olarak uymaları gereken yasal çerçeveyi ve ve buna uyumun nasıl sağlanacağını belirlemiştir. Maddede bahsi geçen komitenin rolünü anlamak için yasalaşma öncesinde kanun tasarıda yer alan genel gerekçeyi incelemek faydalı olacaktır. Gerekçede yer alan ifade aşağıda aynen verilmiştir;

"Tasarı ile kurumsal yönetim ilkelerine uygun olarak, risklerin erken teşhisi ve yönetimi komitesinin kurulması, payları borsada işlem gören şirketlerde zorunlu hale getirilmiştir. Bu komite gerçekte denetim komitesi ve iç denetim komitesinden farklıdır. Ancak her iki komite aynı komite de birleştirilebilir. Türkiye açısından iç denetim komitesinin yanında risklerin erken teşhisi ve yönetimi komitesi özel bir önem

taşımaktadır. Çünkü ülkemizde birçok şirket, faizlerdeki sık dalgalanmalar, devlet bonolarıyla ve tahvilleriyle yapılan işlemler, yatırımların kredilerle finanse edilip, öz varlık / yabancı para rasyosuna dikkat edilmemesi, döviz üzerine spekülasyon yapılması ve özellikle dövizde açık pozisyon vb. sebeplerle doğrudan ve ciddi risk altındadır. Sanayileşmiş, gelişmiş ve istikrarlı ülkelerde pek rastlanılmayan bu tür riskler Türk şirketleri yönünden darboğaza girme ve hatta iflas tehlikesini kolaylıkla beraberinde getirebilmektedir. Kurumsal yönetim ilkeleri arasında bulunmayan bu komiteyi yukarıda açıklanan sebeplerle Tasarı gerekli görmüştür."

TTK'nın "Risklerin Erken Saptanması ve Yönetilmesi" ile ilgili 378.maddesine maddeye ilişkin gerekçe kısmında ise aşağıdaki ifadeler yer almaktadır:

"Hüküm, hisse senetleri borsada işlem gören şirketlerde kurumsal yönetim ilkelerinin bir uygulamasıdır. Tüm anonim şirketler için öngörülmüş bulunan finans denetimi ve denetim komitesine ek olarak yeni bir iç kontrol mekanizmasıdır. Bu komitenin denetim komitesinden farkı denetim komitesinin yönetiminin gözetim altında tutulmasına karşılık bu komitenin sadece risklere odaklanmasıdır. Ayrıca denetim geçmişe yönelik bir inceleme olduğu halde, risk teşhisi gelecek ve geleceğin yorumuyla ilgilidir. Denetimin yönetilmesi söz konusu olmadığı halde risk yönetilebilir ve yönetilmelidir. Amaç burada yönetimi, genel kurulu ve yönetim kurulunu genel bir uyanıklık altında tutmak, gereğinde organlarca derhal etkili önlemlerin alınmasını sağlamaktır. Bu sebeple komite sorumluluk sisteminin merkezinde yer alır. Kanun erken uyarı sistemine (early warning system) istisnai bir önem verdiğinden bu konuda denetçileri de özel olarak görevlendirmiştir. Tehlikelerin erken teşhisi komitesi, bazı yönetim kurulu üyelerinin görevlendirilmeleri suretiyle kurulabileceği gibi, tamamen üçüncü kişilerden de oluşabilir. Komitenin yönetim kurulu üyelerinden meydana gelmesi veya bu üyelerden bazılarının da komitede bulunması halinde ABD'de geçerli olan board sisteminde executive/non-executive üye ayrımına benzer bir durum ortaya çıkabilir. Denetçinin bir diğer önemli görevi de gereklilik ortaya çıktığı takdirde komitenin kurulmasını, hisse senetleri borsada işlem görmeyen bir şirketten de istemesidir. Hüküm bu suretle kurulan komitenin ilk raporunu ne zaman vereceğini de belirtmiştir. Komitenin iki ayda bir yönetim kuruluna hükmün amacına ve ruhuna uygun rapor vermesi gerekir. Kanun tehlikelerin erken teşhisi komitesine aynı zamanda bir iç denetim komitesinin görevlerini de yüklemektedir. Bu sebeple halka açık şirketlerde bu komitenin bir tarafsız yönetim kurulunun başkanlığında çalışması doğru olur. Diğer taraftan kurumsal yönetim kuralları uyarınca kurulması gereken "atamalar komitesi" ile ücretler-finansal haklar-menfaatler komitesine kanun yer vermemiştir. Bunun sebebi tarafsız üye uygulamasında olduğu gibi, bu iki komitenin de Sermaye

Piyasası Kurulu tarafından kurulması gerektiğidir. Çünkü her iki komite de pay senetleri borsada işlem gören anonim şirketler için önerilmiştir. Komiteleri bütün anonim şirketlere teşmil eden uygulama henüz dünyada mevcut değildir."

TTK Md.398, Fıkra (4)'te ise şu cümle yer almaktadır:

" Denetçi, yönetim kurulunun şirketi tehdit eden veya edebilecek nitelikteki riskleri zamanında teşhis edebilmek ve risk yönetimini gerçekleştirebilmek için 378inci maddede öngörülen sistemi ve yetkili komiteyi kurup kurmadığını, böyle bir sistem varsa bunun yapısı ile komitenin uygulamalarını açıklayan, ayrı bir rapor düzenleyerek denetim raporuyla birlikte, yönetim kuruluna sunar. Bu raporun esasları Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumunca belirlenir."

TTK Md. 402, Fıkra (6)'da da şu ibare yer almıştır: "Denetim çerçevesinde, 398'nci maddenin dördüncü fıkrası uyarınca bir değerlendirme yapılmışsa, bunun sonucu ayrı bir raporda gösterilir."

TTK Md.625 Fıkra (1), şu ibare yer almıştır: "Müdürler, aşağıdaki görevlerini ve yetkilerini devredemez ve bunlardan vazgeçemezler. Aynı fıkranın (e) bendinde ise Küçük limited şirketler hariç, risklerin erken teşhisi ve yönetimi komitesinin kurulması."

TTK Md. 635 (1)'de şu ibare yer almıştır: "397'nci maddenin beşinci ve altıncı fıkrası dışında kalan Anonim şirketin denetçiye ve ve özel denetime ilişkin hükümleri limited şirkete de uygulanır."

Yukarıdaki maddeler uyarınca anonim şirketlerde yönetim kurulunun hazırlamak zorunda olduğu faaliyet raporunda risklere ilişkin bilgi vermesi de hüküm altına alınmıştır. (Schöning, Göğüş, Persteiner, 2018:36)

Bu düzenlemeler birlikte değerlendirildiğinde ülkemizde bağımsız denetime tabi olan tüm anonim şirketlerin (limited şirketler dahil) dolaylı şekilde (ki halka açık olmayanlarda denetçi önerisiyle) veya doğrudan (halka açık şirketlerde zorunlu olarak) riskin erken saptanması yükümlülüğü bulunmaktadır. Yönetim Kurulu'nun şirketi tehdit eden veya edebilecek nitelikteki riskleri zamanında teşhis edebilmesi ve risk yönetimini gereçekleştirebilmesi için TTK Madde 378 de öngörülen sistemi ve yetkili komiteyi kurup kurmadığını, böyle bir sistem varsa bunun yapısı ile komitenin uygulamalarını açıklayan ve değerlendiren denetçi raporunun esasları KGK tarafından 18 Mart 2014 tarihinde 28945 sayılı Resmi Gazetede ilan edilen ilke kararıyla belirlenmiş söz konusu kararın ekinde Riskin Erken Saptanması Sistemi ve Komitesi Hakkında Denetçi Raporuna İlişkin Esaslar belgesi eklenmiştir. Bu düzenleme bağımsız denetçinin

denetim yaptığı şirketin riskin erken saptanması sistemi ve komitesinin tüm önemli yönleriyle TTK'nun 378'inci maddesi çerçevesinde yeterli olup olmadığı konusunda bir görüş bildirmesini gerektirse de riskin erken saptanması komitesi tarafından risklere karşı gösterilen çarelerin yerindeliği ve riskler karşısında yönetim tarafından yapılan uygulamalar bağımsız denetimin kapsamı dışında tutulmuştur.

Riskin erken saptanması komitesinin en önemli görevi, işletmede kurumsal risk yönetim sisteminin kurulması ve sürekli geliştirilmesidir. Türkiye'de halka açık işletmelerin kurumsal risk yönetimine verdikleri önem arttıkça, ilgili komitenin rol ve sorumluluklarının da genişlemesi ve değişmesi öngörülmektedir. (Gacar 2017:133).

Kurumsal risk yönetimi uygulamaları TTK'daki hükümlerde de yer aldığı üzere, ilk olarak finans ve bankacılık sektörlerinde başlamış ve daha sonra diğer sektörler de bu uygulamaları takip etmiştir. Öncelikle halka açık şirketler için gerekli görülen bu komite ve sistem, denetçilerin gerekli görmesi halinde diğer işletmeler içinde uygulanabilmektedir.

2.5.2.2. SPK ve BDDK

SPK'nın 2005 yılında yayınlayıp 2011'de de güncellediği Kurumsal Yönetim İlkeleri'nde özellikle yasal mevzuattan kaynaklanan risklerin tespit edilip Yönetim Kurulu'na raporlanması gerektiğine yönelik ifadeler yer almaktadır. Vurgulanan risk grubu yasal riskler olmasına rağmen, günümüz uygulamasında işletmelerin tüm risklerini değerlendirmeleri ve bunları takip edebilmek için etkili bir risk yönetimi sistemine sahip olmaları çok büyük bir gerekliliktir. Sözkonusu ilkelerde kısaca Yönetim Kurulu'nun alacağı stratejik kararlarında risk ve getiri dengesine dikkat etmesi gerektiği, şirketin uzun vadeli hedeflerini göz önüne alarak etkili bir risk yönetimi anlayışı benimsemesinin ne kadar önemli olduğu, başta hissedarlar olmak üzere tüm menfaat sahiplerini doğru bilgilendirmek adına da iç kontrol mekanizması çerçevesinde uygun risk yönetimi sürecinin tanımlanmasının sağlanması ve Yönetim Kurulu'nun yılda en az bir kere tüm bu sistemleri denetimden geçirmesinin gerekliliği ifade edilmiştir. (Resmi Gazete 2011, No:28158)

BDDK'nin risk yönetimine yönelik düzenlemelerinin temeli aşağıda bahsi geçen maddelerde yer almaktadır.

Bankalar Kanunu, 23. Maddesinde; "İç kontrol, risk yönetimi ve iç denetim sistemlerinin ilgili mevzuata uygun olarak tesis edilmesi, işlerliğinin, uygunluğunun ve yeterliliğinin sağlanması, finansal raporlama

sistemlerinin güvence altına alınması, banka içindeki yetki ve sorumlulukların belirlenmesi yönetim kurulunun sorumluluğundadır." şeklindeki ifade ile sorumluluğun tamamen yönetim kuruluna verildiği belirtilmiştir. İlgili kanunun 29. Maddesinde ise; "Bankaların maruz kaldıkları risklerin izlenmesi, kontrolün sağlanması, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tabi ortaklıklarını kapsayan yeterli ve etkili bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlüdür." denilmiştir.

Genel olarak tüm bu uygulamaların, Basel II düzenlemelerine geçişi kolaylaştırmak ve uyumu sağlamak amacıyla da gerçekleştirildiği bilinen bir gerçektir.[*]

2.6. Geleneksel Risk Yönetiminden Kurumsal Risk Yönetimine Geçiş ve Farklılıkları

Geleneksel risk yönetimi sürecinde riskler genellikle kötü olaylar olarak görülmekteydi. Bu nedenle de bu kötü olayları azaltmaya çalışmaktan daha iyi alınacak aksiyon olmadığı görüşü hakimdi. Riskleri azaltırken de sigortalama vb.yöntemler kullanılıyordu. Riskler tek tek değerlendirilmekte ve raporlanmakta idi. Bu da hem zaman hem maliyet kaybı anlamına geliyordu. Tüm bu negatif yanların ortadan kaldırılması için yeni bir risk yönetimi anlayışı benimsenmeye başlandı. (Kızılboğa 2012:303)

Geleneksel risk yönetimi bakış açısına göre tehdit olarak görülen ve bu nedenle azaltılması gereken bir durum olarak düşünülen risk kavramı, günümüzün değişen koşullarında kurumsal risk yönetimi bakış açısı ile sadece riskleri değil aynı zaman da fırsatları da içinde barındıran ve azaltılmasından ziyade en uygun risk stratejisinin belirlenip uygulanması ile yönetilmesi gereken ve bu sayede işletmelerin amaçlarına ulaşmasına, faaliyetlerini verimli bir şekilde gerçekleştirmesine olanak sağlayan bir kavram olarak görülmektedir. Ayrıca kurumsal yönetim, stratejik yönetim, sürdürülebilir büyüme, işletme performansını yükseltme, katma değer yaratma gibi kavramların öneminin artmasıyla birlikte klasik yönetim anlayışından uzaklaşan işletmeleri risk yönetim sistemlerini de yeniden yapılandırmaları gerekmiştir. Zaten geleneksel risk yönetiminin kurumsal risk yönetimine evrilmesinin de en önemli

[*] Ülkemiz, 25 Mayıs 2009 itibarıyla Basel Komite üyeliğine kabul edilmiştir. Komite standartlarına uyum sağlanacağı Ülkemizin de üyesi olduğu G-20 düzeyinde de taahhüt edilmiştir. Komiteye üyelik sonrası BDDK, Komite'nin pek çok alt çalışma grubuna katıım sağlamakta ve Komite tarafından oluşturulan uluslararası standartların oluşturulması sürecine dâhil olmakadır. Komite tarafından kabul edilerek Ocak 2013'te yayımlanan Statü'nün (Basel Committee Charter) 5 inci Maddesi uyarınca Komiteye üye ülkelerin yayımlanan standartları uygulaması gerekmektedir. (bakınız: https://www.bddk.org.tr/Sss/Liste/108)

sebepleri bu bakış açısısındaki değişiklikler ve farklı yönetim ihtiyaçlarıdır. (Usman 2020: 2511)

İşletmelerin operasyon alanlarının zamanla genişlemesi ve bu büyümenin etkisiyle işletmeden faaliyetlerinden menfaat beklentisi içinde olan ilgililerin sayısı da artmıştır. İş dünyasında işletmelerin tüm paydaşlarının, hissedarlarının ve ilgili her kişinin/kurumun beklentilerinin karşılanabilmesi ve işletmenin sürdürülebilirliğinin devamı için etkili bir risk yönetimi sistemini kurmuş olması ve uygulaması gerekmektedir. Bu ihtiyaç geleneksel risk yönetiminin kurumsal risk yönetimi olarak evrilmesi sonucunu doğurmuştur. (Beasley, 2005: 522). Kurumsal risk yönetimine geçiş sürecinde birçok işletme farklı danışmanlık firmalarından kurumsal risk yönetimi sisteminin kendi bünyelerinde kurulabilmesi için destek almışlar ve akademik dünyada da üniversiteler, kurumsal risk yönetimi kavramına yönelik konuları ders içeriklerine eklemeye başlamışlardır. (Lienberg ve Hoyt, 2003: 37)

Geleneksel risk yönetiminde birim, bölüm bazında risklere yönelik alınan kararların farklı bir alanda başka risklere sebep olması hali, kurumsal risk yönetimine geçiş ile ortadan kaldırılmıştır. (Beasley, Branson ve Hancock 2008: 45). İşte tam da bu noktada, geleneksel risk yönetiminden kurumsal risk yönetimine geçiş, risklerin birbirlerinden bağımsız ve münferit olarak değerlendirilmesi anlayışından vazgeçip artık risklerin ve hatta fırsatların bir bütün olarak yönetildiği bütünleşik, sistematik, yeni bir süreç yönetimine geçişi ifade etmektedir. Tabii geleneksel risk yönetiminin genelde riski azaltma yoluna gitmesi ve bu yöntemin de işletmenin operasyonlarına sekte vurması sebebiyle geleneksel bakış açısı zamanla yerini kurumsal risk yönetimi anlayışına bırakmıştır.

Kurumsal risk yönetiminde proaktif bakış açısı benimsenmektedir. Proaktif bakış açısı ile çeşitli detaylı analiz teknikleri ile risklerin tespit edilmesi, ölçülmesi, değerlendirilmesi aşamalarının sağlıklı şekilde yerine getirilmesi ve bu sayede riskin yönetiminin mümkün kılınmasıdır. Bu bakış açısında, her riskin bir fırsat, her fırsatın da bir risk içerdiği varsayımı önem kazanmıştır.

Bu süreç tabii ki işletme açısından bir dönüm noktasını ve çok önemli bir dönüşümü ortaya koymaktadır. Bu dönüşüm birbirini takip eden çok sayıdaki sürecin uygulanmasını gerektirir. Dönüşümün başarılı olmasında işletmenin üst yönetiminin olduğu kadar işletmede çalışan her bireyin çok ciddi katkısı olacaktır. Ancak işletme genelinde farkındalık oluşursa ve genel katılım sağlanır ise bu tarz değişimlerin başarı getirmesi kaçınılmaz olur.

Aşağıdaki tabloda geleneksel risk yönetimi ile kurumsal risk yönetimi arasındaki farklılıklar özetlenmiştir.

Tablo 3. Geleneksel Risk Yönetimi ile Kurumsal Risk Yönetiminin Karşılaştırılması

Faktörler	**Risk Yönetimi**	**Kurumsal Risk Yönetimi**
Perspektif	Riskler	Risk ve fırsatlar
Odak	Belli başlı operasyonlar	İşletmenin tamamı ve paydaşları
Sorumlular	Bazı yöneticiler	Herkes
Detay seviyesi	Çok ayrıntılı analizler	Genel değerlendirmeler
Zamanlama	Düzenli	Sürekli
Dil	Benzer terimler ama farklı perspektifler	Ortak dil ve perspektif
Raporlama	Parça parça raporlama	Entegre ve bütünsel raporlama
Kontrol Odağı	Bireysel kontrol mekanizması	Bütünsel kontrol çerçevesi
Hedef	Risklerin yönetimi	Hedeflere ulaşmak ve katma değer yaratmak için risk ve fırsatların yönetimi
Kapsam	Operasyonel	Stratejik
Standart	Yöneticiye bağlı	Yönetim kurulunun belirlediği yönergeye bağlı
Vizyon	Üst yönetimi korumak	İşletmenin değerini ve itibarını artırmak

Kaynak: Pickett, 2005:77

Yukarıdaki farklılıklar göz önüne alındığında, geleneksel risk yönetiminde sadece risklerin tek tek değerlendirildiğini, roller ve sorumlulukların pek net olmadığını, risk kültürü ve farkındalığının işletmede mevcut olmadığını görülmektedir. Tam tersi yönde de kurumsal risk yönetiminde riskler ve fırsatlar bütünleşik olarak değerlendirilmektedir, sürecin sorumluları, rolleri belirgindir. Risk kültürü işletmede mevcuttur, risk farkındalığı ise her seviyede oluşturulmuştur.

Kurumsal risk yönetiminde işletme yöneticileri ellerinde sınırlı kaynakları en doğru şekilde kullanmaya/yönetmeye çalışmaktadırlar. Yöneticiler riskleri bütünleşik olarak değerlendirmeye tabi tutarlar ve takiplerini de bu bakış açısıyla yapmaktadırlar. Böylece farklı stratejiler geliştirilebilmekte, çok boyutlu düşünerek çeşitli önlem planları yapılabilmektedir.

Kurumsal risk yönetim sistemi, geleneksel risk yönetimindeki gibi riskleri kaçınılması gereken olaylar olarak algılamaz, risklerin yönetilip işletme için değere dönüştürülebileceği varsayımıyla ilerlemektedir. Burada ilgili süreçte, yalnız finansal tabloların kontrolü ya da mevzuata uygunluk hedefleriyle değil, işletmenin tüm faaliyet alanlarıyla ilgili hedeflere odaklanılmaktadır. (Kızılboğa 2012:312)

Kurumsal risk yönetiminin bir şirkette uygulanabilmesi için öncelikle bazı ön şartların oluşması gerekir. Bunların başında yer alan noktalar aşağıda sıralanmıştır:

- İşletmenin organizasyon yapısı kurumsal risk yönetiminin uygulanmasına müsaade edecek şekilde olmalıdır.
- İşletmedeki iç kontrol süreçleri oturmuş olmalı, roller ve sorumluluklar net bir şekilde tariflenmelidir.
- İşletmenin yönetim ve denetim mekanizması kurumsal risk yönetimi süreci ile uyumlu hale gelmeli ve bu sürecin ayrılmaz bir parçası olmalıdır.

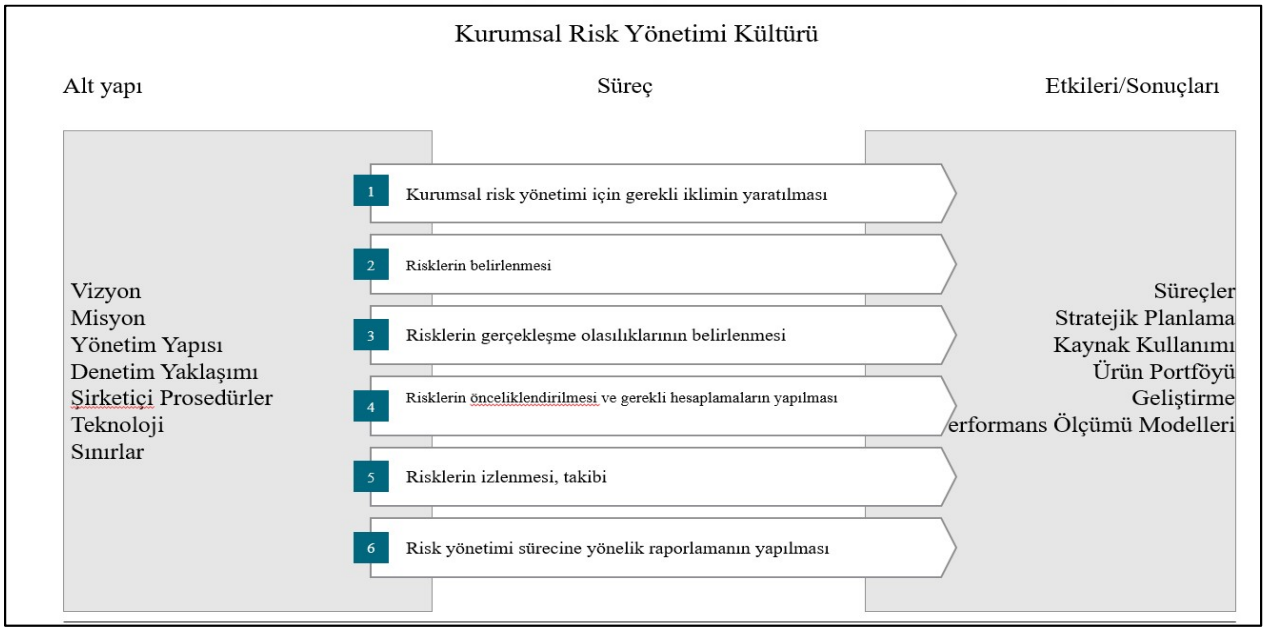
İşletmede kurumsal risk yönetiminin uygulanabilmesi için olmazsa olmaz denilebilecek olan kavram risk kültürüdür.

İşletmelerin kendi kültürleri ile risk kültürü arasındaki ilişkiye yönelik olarak 2012 senesinde Risk Yönetim Enstitüsü tarafından bir çalışma gerçekleştirilmiştir. Bu araştırmada, işletmelerin risk kültürünün gelişiminin sağlanması için Kurumsal Risk Yönetimi'ne (KRY) yönelik çalışmaların yapılması gerektiği ve ancak kuvvetli kültüre sahip işletmelerde risk yönetiminin gelişim gösterebileceği ifade edilmiştir.

İşletmelerde risk yönetiminin oturtulmasında en önemli geliştirilmesi gereken yanlardan biri, işletmenin riskli olaylara yönelik hareket tarzlarının ve bunun işletme içindeki risk yönetimini nasıl etkilediğininin doğru anlaşılmasıdır. Bu noktadan sonra yapılması gereken tüm doğru tutumların risk kültürü olarak işletmeye yerleşmesinin sağlanması olacaktır. (The Institute of Risk Management, 2012, 6-11)

Risk and Insurance Management Society (RIMS)'ye göre de risk kültürü, bir anlamda işletmede çalışanların risklere yönelik farkındalık düzeyinin yüksek olması ve işletme içindeki tüm risk yönetimi sürecinin bu bilinç düzeyine uygun şekilde tasarlanması olarak da tanımlanabilmektedir. İşletmede mevcut olan risk kültürü, stratejik risk yönetim kapasitesini ve işletmenin amaçlarına ulaşabilmesini doğrudan etkilemektedir. Risk kültürünün işletmede doğru şekilde yerleştirilmemiş olması, üst yönetimin aldığı kararların birbirleri ile ve prosedürlerle uyumlu olmamasına, çalışanların işletmede karşılaştıkları uygunsuz durumlara ses çıkarmamasına ve dolaylı olarak işletmenin itibar kaybetmesine sebep olabilmektedir. (The Institute of Risk Management, 2012: 8).

Konuyu bütünsel olarak inceleyebilmek için risk kültürünün sisteme oturtulmasına yönelik tüm etkenler (Şekil 2)'de şematik olarak gösterilmiştir.



Şekil 2. Kurumsal Risk Yönetimi Kültürü

Kaynak: Yazar tarafından oluşturulmuştur.

Yukarıdaki şekilde görsel olarak ifade edildiği üzere, kurumsal risk yönetimi sürecine geçilmek istendiğinde, öncelikle şirketin vizyonu ve misyonu bu doğrultuda güncellenir, yönetim yapısı ve tabii ki iç kontrol ve iç denetim yaklaşımları incelenir, prosedürlerde gerekli düzenlemeler yapılır. Bu şekilde alt yapı hazırlığı tamamlanmış olur. Sonrasında ise kurumsal risk yönetimi sürecinin adımları sırasıyla uygulanır ve neticede de önceki uygulamalara nazaran çok daha verimli iş süreçlerine ulaşılmış, planlama adımları ile entegre edilmiş, piyasa/pazar koşullarına daha kolay uyumlanabilen ve kendini ürün gamı anlamında da güncelleyebilen bir yapıya geçilmiş olur. Şeklin sol tarafında gördüğümüz temalar bize aslında yapılan hazırlıkları ifade ederken sağ tarafta da ulaştığımız nokta gösterilmektedir.

Hazırlık aşamasında işletmenin var olan risk yönetimi süreci ile yeni kurgulanan sistem arasındaki farklar incelenmeli ve ortaya konulmalıdır. Bu şekilde kurumsal dönüşüm sürecinde yapılması gerekli olacak değişimlerin bir listesi çıkarılıp onun üzerinden yürünebilmektedir. Bu aşamadan sonra, işletmenin hedeflerinin gözden geçirilmesi ve şu ana kadar göze aldığı risklerin ayrıntılı bir şekilde incelenmesi gerekmektedir. Bu şekilde kurumun risk iştahı, limitleri, neleri yapabileceği daha rahat ortaya çıkarılabilmektedir. Önceki yıllarda dikkate aldığı ve stratejisini ona göre yönlendirdiği tüm riskler, işletmenin aslında risk alma konusundaki hevesinin ve varsa bu konudaki kısıtlarının anlaşılmasına destek olmaktadır. Mevcut durumun anlaşılmasından sonra amaçlanan kurumsal risk yönetimi süreci tasarlanmaya başlanır. Bu çalışma sırasında işletmenin büyüklüğü, ait olduğu sektör, personel politikası ve mevcut durum analizinde ortaya çıkan diğer parametreler dikkate alınır. Bu noktadan sonra artık dönüşüm başlar.

Dönüşüm başladığında ilk yapılması gereken şey işletmede risk kültürünü yerleştirmek ve organizasyonun her adımında risk farkındalığının yerleşmesini sağlamaktır. Zaten dönüşümde en çok zaman alacak olan adımda burasıdır. Kurumsal risk yönetimine uygun kurum kültürünün işletmede oluşturulması meşakkatli bir süreçtir. Hedeflenen yapının oluşturulmasındaki en önemli faktörler aşağıda yer almaktadır:

- Üst yönetimde yer alan yöneticilerin kurum kültürünün değiştirilmesine yönelik yoğun istek duyması
- Kurulacak yeni sistemin işletmeye uzun vadede faydalı olacağına yönelik inancın varlığı
- İşletmede kurumsal risk yönetimi sürecinin uygulanıp takip edilmesini sağlayacak bilgi teknolojileri yatırımının yapılması ve kurulacak olan sistemin tespit edilen risklerin uzun dönemli takip edilip raporlanmasına imkan sağlaması.

- Risk yönetimi sürecinin şirket içinde uygulanmasını organize edecek, gerekli iç kontrol adımlarını gerçekleştirecek yeni bir birimin oluşturulması ve bu birimin düzenli aralıklarla üst yönetime rapor vermesinin sağlanması.
- İşletmenin her bölümünde risklerin tespit edilip gerekli adımların atılmasını sağlayacak, sürekli olarak süreci takip edecek ve risk yönetimi bölümüne bildirimde bulunacak risk uzmanlarının belirlenmesi ve gerekli süreç eğitimlerinin tamamlanması.
- Çalışanların performans yönetimi araçları aracılığıyla kurumsal risk yönetimi sürecine katkı sağlamasının özendirilmesi.
- Risk yönetimi sürecinde kullanılacak olan terminolojinin, el kitaplarının, risk kataloğunun, çalışanlara verilecek olan eğitimlerinin içeriğinin ve dokümanlarının hazırlanması.
- Gelişmeye açık ve sağlıklı yapılanması olan işletmelerde risklerin sıfırlanmasının mümkün olmadığı, hedefin riski en aza indirmek olması gerektiği konusunda işletme içi farkındalığın sağlanması.

Yukarıdaki tüm etmenlere dikkat edilirken, risk yönetimi uygulamalarının en önemli gayesinin üst yönetime erken uyarı sistemi içerisinde proaktif davranarak geri bildirimlerde bulunulması olduğu unutulmamalıdır. Kurumsal risk yönetiminin tek başına bir süreç olmadığı, bir süreçler silsilesi olduğu ve süreklilik arz etmesi gerektiği unutulmamalıdır. (Bakkal, Kasımoğlu, Tunç 2016:81-85)

2.7. Kurumsal Yönetim Kavramı

Yönetim, bir grup insanın ortak bir amaç doğrultusunda yönlendirilmesi, onlara liderlik edilmesi, onların çabalarının bir işbirliği haline getirilmesi ve denetlenmesidir. (Ergun 2004:63).

Kurumsal Yönetim konusuna yönelik çalışmalar 1980'lerin başında başlamıştır. O dönemlerde ve öncesinde ABD'de bazı büyük şirketlerin üst düzey yöneticilerinin sadece işletmenin karını maksimize etmeye yönelik hareket etmeleri, hissedarlar veya diğer paydaşların menfaatlerini yeteri kadar gözetmemeleri, işletmenin sürdürülebilirliğine yönelik çalışmalar yapmamaları ve hatta bu konuya pek ehemmiyet vermemeleri sebebiyle birçok bilinen şirketin (Enron, Bristol-Myers, Squibb, Qwest, Xerox, WorldCom vb.) iflas ettiği, operasyonlarını durdurmak durumunda kaldığı elim olaylar yaşanmıştır. Tüm dünyada yankı uyandıran bu gelişmelerden sonra kurumsal yönetim (yönetişim) kavramı günden günde değer kazanmaya başlamıştır. Yaşananların yansıması ve neticesi olarak; şeffaflık, gerçeklik, adalet, doğru

ve zamanında bilgilendirme gibi kurumsal yönetimin temellerini oluşturan değerlere işletmeler kıymet vermeye ve günlük operasyonlarını bu değerlere göre yönetmeye başlamışlardır. (Karaca, Şenol, Korkmaz 2018: 236).

İşletmelerin hem başarıya ulaşıp hem de sürdürülebilirliği devamlı hale getirebilmesi için etkili şekilde yönetilmeleri ve günümüzün değişen koşullarına uyum sağlayabilmeleri gerekir. Geleneksel yönetim yaklaşımları artık işletmelerin etkili şekilde yönetilebilmesi için yetersiz kalmaktadır. Yeni dönemdeki mali piyasalarda her gün farklı kavramlar ortaya çıkmakta ve var olan kavramlarda zaman içinde sürekli değişim göstermektedir. Global dünyada gerçekleştirilen ticaret beraberinde birçok kazanım getirmiş olsa da finansal piyasalarda zaman zaman krizler ortaya çıkmakta, işletmelerin paydaşlarının ihtiyaçlarını karşılamak üzere hazırlanan mali tablolardaki bilgilerin güvenilirlikleri de sorgulanır hale gelmektedir. Neticede, ülkelerin daha yüksek refah düzeyine ulaşmasının ve kalkınmasının en temel aracı işletmelerdir. İşletmelerin, sosyal sorumluluk ve etik değerler çerçevesinde adaleti, şeffaflığı ve hesap verilebilirliği sağlamak için kurumsal yönetim uygulamalarına ciddi önem vermeleri gerekmektedir. (Karcıoğlu, Kurnaz, Güner 2019: 104).

İşletmeler çevrelerindeki diğer ekonomik, siyasal ve sosyal organizasyonlarla uyumlu şekilde ilişkilerini sürdürmelidir. Bu organizasyonel gruplar; işletmenin müşterileri, tedarikçileri, rakipleri, hissedarları, beraber çalıştığı finansal kurumlar, kamu kurumları olabilir. Bu grupların herbirinin işletme ile ilgili kendine özgü hedefleri vardır. Kurumsal yönetim anlayışı içinde tüm bu gruplar birbirleriyle etkileşim içinde hayatlarına devam etmektedirler. (Vasile & Simon 2019: 10).

1990'lı yıllara gelindiğinde artık kurumsal yönetim kavramının yanına risk yönetimi kavramı da eklenmiştir. Bu şekilde işletmeler risk yönetimi sistemi ile bünyelerindeki riskleri yönetme imkanına kavuşmuşlardır. 2000'li yılların başından itibariyle de artık risk yönetimi kurumsal risk yönetimi olarak yoluna devam etmiştir. Entegre yani bütünleşik kurumsal risk yönetimi sistemi aracılığıyla, işletmeler hedeflerini, stratejilerini oluşturmaya, risklerini ve buna ek olarak fırsatlarını takip edip yönetmeye başlamışlardır. Vizyon, misyon, strateji kavramları hiç olmadığı kadar konuşulmaya ve üzerinde çalışılmaya başlanmış ve kurumsal risk yönetimi ile iş hayatının gündemine "katma değer" yaratan süreçler de dahil olmuştur.

Kurumsal yönetim veya yönetişim, son yirmi yıldır literatürde popüler hale gelmiş bir kavramdır. En basit tanımıyla "organizasyonların yönetildiği ve kontrol edildiği yoldur". Kurumsal yönetim işletmelerin hedefledikleri performansa ulaşmalarını denetleyen ve aynı zamanda işletmelerin standartlara, kurallara, yönetmeliklere, politika ve prosedürlere bağlı kalıp kalmadıklarını da kontrol eden karışık bir sistemdir. Kurumsal yönetim aynı zamanda organizasyonların iç denetim fonksiyonunun sistem içindeki etkililiğini değerlendirmesine olanak sağlayan yapıyı da ifade etmektedir. (Korkmaz 2020: 182).

OECD tarafından ortaya konulan tanıma göre yönetişim, bir işletmenin üst düzey yöneticileri, yönetim kurulu, hissedarları ve diğer paydaşları arasındaki ilişkiler bütünüdür. Kurumsal yönetim aynı zamanda işletmenin hedeflerinin belirlendiği, bu hedeflere ulaşmadaki performansın değerlendirilebilmesi için gerekli araçların tanımlandığı bir bütünsel yapıyı anlatmaktadır.

Uluslararası İç Denetçiler Enstitüsü (IIA) ise kurumsal yönetim kavramını; "Yönetim kurulu, her seviyeden yöneticiler ve denetim kurulu tarafından işletmenin hedeflerine ulaşmasına yönelik olarak tüm faaliyetlerinin raporlanması, yönlendirilmesi, yönetilmesi, izlenmesi amacıyla uygulanan yapı ve süreçlerin birleşimidir" şeklinde açıklamaktadır.

Kurumsal yönetim ekonomik krizlere karşı bir koruyucu olarakta tanımlanmaktadır. Ülkelerin yönetişim prensiplerini uyumlu hale getirmelerinin ana sebebi, ekonomik iniş ve çıkışlardaki potansiyel risklerden kendilerini koruma çabasıdır. (Muneeza ve Wajeeh, 2012:203)

Stratejik yönetim ise, işletmenin geleceğe ilişkin hedeflerinin saptanıp bunlara ulaşabilmek için yapılması gerekenlerin adımların belirlenmesine olanak sağlar. (Ergun 2004: 71). Stratejik yönetim kavramının içinde işletmenin sahip olduğu kaynakları ve dış çevredeki riskleri/fırsatları yönetmekte yer almaktadır. Bu anlayış zamanla kurumsal risk yönetimi kavramını ortaya çıkarmıştır. Aynı şekilde işletmelerin modern bir anlayışla yönetilmesi düsturu içerisinde günden güne farklılaşan toplam kalite yönetimi anlayışı da mevcuttur. (Karaman, Tosuner 2020: 99).

2.7.1. Kurumsal Yönetimin Amacı ve İlgili Teoriler

Mevcut ekonomik düzende, işletmelerin birbirleriyle sıkı rekabetleri sonucunda kurumsal yönetim kavramının önemi artmıştır. Kurumsal yönetim; işletmelerin her durumda operasyonlarına devam etmesini

sağlayan yönetsel politikalar olarak tanımlanmaktadır. Aynı zamanda kurumsal yönetim, işletmelerin verimliliğini artırmayı ve tüm paydaşlarıyla ilişkisini düzenlemeyi de hedeflemektedir. (Radu, 2012: 114)

ICAEW'e (Institute of Chartered Accountants in England and Wales) göre, kurumsal yönetimin amacı, işletmelerin uzun vadeli başarısını sağlayabilecek etkili, girişimci ve basiretli yönetimi kolaylaştırmaktır.

Kurumsal yönetim kavramı olumlu-olumsuz anlamda dört temel teori ile ilişkilidir. Bunlar vekâlet teorisi, işlem maliyetleri, paydaş ve hizmetkârlık teorileridir. Vekalet teorisinde yöneticiler ile hissedarlar arasında "Vekâlet İlişkisi" mevcuttur. Bu ilişkide yöneticilerden beklenen hissedarlardan aldıkları yetkileri yine hissedarların menfaatine kullanmaları gerekir. Burada doğal olarak karşımıza vekil maliyeti kavramı çıkmaktadır. Vekil maliyeti, yetkiyi hissedardan alan yöneticinin görevini yaparken kendi menfaati ile hissedarın menfaati arasında kalmasının sonuçlarını ifade etmektedir. İşlem maliyetleri teorisine göre ise, işletmeler beklenti ve hedefleri farklı olan kişilerden kurulmuş organizasyonlardır. Yöneticiler menfaatçi yaklaşımdadırlar ve kendi çıkarları için işletmenin verilerini manipüle edebilirler. Bu teoriye göre, işletme bünyesinde dürüstlük, ahlaki değerler, yönetişim prensipleri, şeffaflık, hesap verilebilirlik ve sorumluluk ilkelerine dayanan bir yönetişim yapısının kurulabilmesi pek mümkün değildir. Paydaş teorisine göre, günümüzdeki işletmelerin hacmi genellikle büyüktür ve toplum üzerindeki etkisi de oldukça fazladır. Bu yüzden de işletmelerin yönetiminde yer alan yöneticilerin sadece kendi hissedarlarına karşı değil aynı zamanda işletmenin yer aldığı eko sistemdeki tüm çıkar gruplarına karşı sorumluluk duymaları gerekir. Buradaki çıkar grupları arasında tedarikçiler, yatırımcılar, müşteriler, çalışanlar yer alımaktadır. Hizmetkâr teorisinin özünde de, yöneticilerin işletmenin hizmetkârları olarak hissedar değerini ve zenginliğini artıracak biçimde görevlerini özenli şekilde gerçekleştirmeleri yer almaktadır. Bu teoride, hissedarlar yöneticilerine güvenirler ve onların işlerini iyi yaparak işletmenin karını sürekli artıracaklarına inanırlar. Her iki taraf da bu ortak amaç etrafında birlikte çalışarak güçlü bir yönetişim sürecine katkı sağlamaktadırlar. (Korkmaz 2020: 183-184).

2.7.2. OECD'nin Kurumsal Yönetimin İlkeleri

Yukarıda da değinildiği üzere, kurumsal yönetim dünyada 600 yıldır tartışılan ve geçmişi olan bir kavramdır. 1990'ların sonu ve 2000'li yılların başında oldukça önem kazanmış ve bu konuda çeşitli girişimler yapılmaya başlanmıştır. Tüm bunların ortaya çıkmasında o yıllarda dünyaya çok görülen skandalların da etkisi olmuştur. (TKYD, 2023:12)

Kurumsal risk yönetiminin ilkeleri denildiğinde ilk akla gelen OECD'nin 1999 yılında hazırlayıp yayımladığı "OECD Kurumsal Yönetim İlkeleri" akla gelmektedir. Bu çalışma, kurumsal yönetim anlayışını uluslararası bir yapıya kavuşturmak üzere yapılan ilk çalışmadır. Sözkonusu ilkeler daha sonrasında ülkelerin kendilerine özgü olarak hazırladıkları düzenlemelere temel teşkil etmiştir. Ayrıca ilkeler, işletmelerin menkul kıymetlerinin işlem gördüğü borsalar, tüm yatırımcılar ve ilgili diğer kuruluşlara uygulanabilir öneriler sunmaktadır. OECD'nin kabul ettiği bu kurumsal yönetim ilkelerinin amacı; OECD'ye üye olsun veya olmasın kurumsal yönetimi ülkesinde uygulamak, yaygınlaştırmak amacında olan, bu yönde yasal düzenlemeler, uygulamaya yönelik çalışmalar yapan, yapmak isteyen ülkelere, devlet yönetimlerine yardımcı olmak ve yol göstermektir. (TKYD, 2004:4) OECD, 2004 yılında kurumsal yönetim ilkelerini gözden geçirip düzenlemeler yapıp tekrar yayınlamıştır.

OECD'ye göre kurumsal yönetim, ekonomik büyümeyi artırırken aynı zamanda da yatırımcı güveninin kazanılmasının en önemli öğelerinden biridir. Kurumsal yönetim, bir işletmenin yönetimi/hissedarları ve tüm paydaşları arasındaki iletişimi de kapsamaktadır. Bu kavram, aynı zamanda işletmenin hedeflerinin/stratejilerinin belirlendiği bir düzeni oluşturmakta ve tüm bunlara nasıl ulaşılacağına yönelik anahtarlar da sunmaktadır. (TKYD, 2004:9)

Bu alanda Türkiye'de de 2002 yılında TÜSİAD "En İyi Uygulama Bilgilendirme Kitapçığı" nı yayınlamış ve sonrasında da 2003'te Sermaye Piyasası Kurulu (SPK) tarafından "Kurumsal Yönetim İlkeleri" açıklanmıştır. Yine aynı kurumsal yönetim anlayışının ülkemizde de hayata geçirilmesi, yaygınlaştırılması amacıyla Türkiye Kurumsal Yönetim Derneği (TKYD) kurulmuştur. TKYD eliyle OECD'nin 2004'te yayınladığı ilkeler Türkçe olarak kamuoyuna sunulmuştur. Sonrasında SPK yine 2005, 2011, 2012, 2014'te yayınladığı tebliğler ile bu konudaki standart ve ilkeleri geliştirmiştir. (TKYD, 2023:13-14)

Kurumsal yönetimin ana dört ilkesi adillik, sorumluluk, şeffaflık ve hesap verilebilirliktir. Diğer bütün detaylar bu maddeler etrafında şekillenmektedir.

İşletmelerin kurumsal yönetim ilkelerini benimsemeleri, verecekleri yatırım kararlarının sağlıklı olabilmesi açısından da önem arz eder. İyi kurumsal yönetimin tek bir modeli yoktur. Ülkelere ve şartlara göre değişkenlik göstermektedir.

Zamanla dünyada meydana gelen ekonomik, politik olaylar ve gelişmeler neticesinde 2004'te yayınlanan kurumsal yönetim ilkelerinin güncellenmesi gerekliliği ortaya çıkmıştır. 2015 senesinde OECD tarafında yine büyük bir mutabakat ile çalışılan yeni kurumsal yönetim ilkeleri yayınlanmıştır.

2014 yılında yayınlanan kurumsal yönetimi ilkelerini aşağıda görebiliriz: (TKYD, 2015:5-6)

- Etkili kurumsal yönetim çerçevesinin temelinin sağlanması: Bu ilkede, kurumsal yönetim çerçevesinin kaynakların verimli bir şekilde dağılmasında büyük rolü olduğu ve kurumsal yönetim uygulamalarında tüm taraflarının görev ve sorumluluk dağılımı üzerinde durulur. Burada denetim kalitesine de vurgu yapılır.
- Pay sahiplerinin hakları ve adil muamele görmeleri ile temel ortaklık işlevleri: Bu ilke, ortakların doğru bilgiye zamanında erişebilmesi ve diğer haklarının korunması üzerinde yoğunlaşır.
- Kurumsal yatırımcılar, pay senedi piyasaları ve diğer aracılar: Bu ilke yeni bir bölümdür, kurumsal yatırımcıların ve diğer tüm aracı firmaların haklarını düzenler.
- Menfaat sahiplerinin rolü: Burada da tüm menfaat sahiplerinin bilgiye kolay erişmesi ve haklarının korunması bahis konusu edilir.
- Kamuyu aydınlatma ve şeffaflık: Kamuya yapılan tüm açıklamaların şeffaf, zamanında ve gerektiği gibi yapılması üzerinde durulur.
- Yönetim kurulunun sorumlulukları: İşletmenin hedef ve stratejilerinin meydana getirilmesi, yönetim kurulunun ve üst yöneticilerin tüm diğer sorumlulukları bu alanda yer alır.

OECD kurumsal yönetim ilkeleri, değişen dünyanın etkisiyle –iki yıllık bir çalışmanın sonunda- 2023 yılında tekrar revize edilmiştir.

2023 yılında gelen revize, kurumsal mülkiyet, yatırımcıların ve yönetimin kurumsallaşmada artan rolü, işletmelerin karşı karşıya olduğu risklerin artması ve risk haritalarının karmaşıklaşması, dijitalleşmenin etkisi sebebiyle bazı güncellemeleri içermektedir. Bunların yanısıra bir de özellikle işletmelerin sürdürülebilirlik ve dayanıklılık üzerine yapması gerekenler, düşünmesi gerekenler gündeme gelmiştir. Buna göre, işletmelerin kurumsal yönetim çerçevelerinin işletmelerin ve dolaylı olarak yaşadığımız dünyanın sürdürülebilirliğine katkı yapması gerektiği vurgulanmıştır. Ayrıca sürdürülebilirliğe yönelik olarak işletmelerin şeffaf, tutarlı ve zamanında bilgilendirmeler yapmaları da kapsam içinde yer almıştır.

Ancak bu anlayış ile ekonomilerin, içinde yaşanan eko sistemin devamlılığının sağlanabileceği belirtilmektedir. (TKYD, 2023: 20).

2.7.3. Kurumsal Yönetimin Faydaları

İşletmelerin büyüyüp gelişmesi, büyümesini daha kolay ve ucuz maliyet ile finanse etme arzu ve isteği halka arz yönünde kararlar alması neticesini doğuracaktır. Aile işletmelerinin halka açılmak suretiyle büyümeleri ve sermaye piyasalarında işlem görmeleri, işletmelerdeki kurumsallaşma ve kurumsal yönetim uygulamalarını geliştirmektedir. Bu yaklaşımlar ayrıca, işletmelerin devamlılıklarına katkı sunarken, firmaların daha uygun şartlarda finanse edilmesini de sağlayabilmektedir (TKYD, 2010: 14).

Kurumsal yönetim uygulamalarının faydaları genel olarak şöyle sıralanabilir:

- Sermaye maliyetinin azalması,
- Finansman olanaklarının ve likiditenin artması,
- Ülke imajının iyileşmesi, yabancı sermaye girişinin artması,
- Yerli sermayenin ülke çıkışına engel olması,
- Sermaye piyasasının gücünün artması,
- Krizlerin rahat atlatılması ile birlikte kaynakların daha etkili kullanılmasına yol açması,
- Müşteri beklentilerine uyum ve yeni pazarlara nüfuz etme gücünün desteklenmesi,
- Hesap verme sorumluluğunu sağlaması,
- Toplum yararının gözetilmesi,
- Doğrudan sermaye yatırımlarının arttırılması (Polat, 2018: 38-39).

2.7.4. Kurumsal Yönetim ve Kurumsal Risk Yönetimi Arasındaki İlişki

Kurumsal risk yönetimi süreci 1990'lı yılların sonlarında kurumsal yönetim kavramının içine entegre edilmiştir. Kurumsal yönetim, kurumsal risk yönetimine göre çok daha eski bir kavramdır.

Kurumsal yönetim ile kurumsal risk yönetimi arasındaki iç içe geçmiş ilişki aşağıdaki Tablo: 4 ve Tablo: 5'de verilmiştir:

Tablo 4: Kurumsal Yönetimin Kurumsal Risk Yönetimi Üzerindeki Etkileri

1	İşletmenin operasyonlarını etkileyen risklerin raporlanmasında şeffaflığın ve kamuya açıklamanın gözetilmesi
2	İşletmenin tüm paydaşlarının beklentilerinin kurumsal risk yönetimi sürecine dahil edilmesiyle etkili bir kurumsal yönetimine ulaşılması
3	İşletmelerde yönetim kurulunun risk yönetiminden sorumlu olması
4	Risklerin belirlenmesi ile karar verilen risk stratejilerinin uygulanması sürecinde gerekli kontrollerin ve denetimlerin gerçekleştirilmesi
5	İşletmedeki risklerin doğru yönetildiğine dair kurumsal yönetimin güvence vermesi

Kaynak: Karaca, Şenol, Korkmaz 2018: 237-238.

Tablo 5: Kurumsal Risk Yönetiminin Kurumsal Yönetim Üzerindeki Etkileri

1	İşletmenin günlük operasyonunda iniş çıkışları ve sürprizlerin en aza indirilmesi
2	İşletmede mevcut risklerin üst yönetime ve diğer yöneticilere raporlanması, risk cevaplarının uygulanmasının sağlanması
3	Risk yönetiminin işletmenin tamamında ve bütünleşik seviyede uygulanması
4	Kurumsal risk yönetiminin iş dünyasında kurumsallaşmayı artırması
5	Kurumsal risk yönetiminin üst yönetim tarafından belirlenen hedeflere ulaşılması yolunda kabul edilebilir bir güvence sağlaması
6	Kurumsal risk yönetimi sisteminin üst yönetimin karar alma süreçlerine dahil edilmesi
7	Kurumsal risk yönetiminin kurumsal yönetimin temel bileşeni olması

Kaynak: Karaca, Şenol, Korkmaz 2018: 237-238.

Yukarıdaki tablolardan anlaşıldığı üzere, kurumsal yönetim her zaman kurumsal risk yönetimi süreci üzerinde bir güvence alanıdır. Bilgi, iletişim, yetkilendirme, kontrollerin gerçekleştirilmesi gibi konularda kurumsal risk yönetimine rehberlik eder. Kurumsal risk yönetimi ise, kurumsal yönetimin en önemli bileşenlerinden biridir. İş dünyasında kurum kültürünün oluşması, yaygınlaşması hep risk yönetimi süreçlerinin desteği ile gerçekleşmektedir. Ayrıca işletmelerin stratejilerinin, hedeflerinin gerçekleştirebilmeleri; bu hedeflere yürürken ortaya çıkabilecek riskleri ve fırsatları ne kadar doğru tespit edip etmediklerine, üst yönetimin karar alma mekanizmasının içine risk yönetiminin ne kadar entegre edilip edilmediğine bağlıdır. Ancak etkili bir kurumsal risk yönetiminin kurulmuş olduğu işletmelerde; işletmenin geleceği daha güvenli bir seyir izler, işletmenin sürdürülebilirliği sağlanır, başarılar/kazançlar uzun dönemli ve tutarlı olur ve işletme vizyonunu, misyonunu gerçekleştirme imkanına kavuşur.

IIA'in de ifade ettiği gibi, risk yönetimi kurumsal yönetimin esas öğesidir. Bir işletmede üst yönetim, etkili risk yönetimi çerçevesini kurmak ve uygulamakla yükümlüdür.

3. İÇ KONTROL SİSTEMİ VE KURUMSAL RİSK YÖNETİMİ SÜRECİ

3.1. İç Kontrol Sistemlerine Genel Bakış

İç kontrol ile ilgili olarak bugün için dünyada en geçerli ve etkili düzenleme ABD'de COSO diye ifade edilen ulusal bir komisyon tarafından yapılmış olup diğer ülkelerdeki düzenleyici otoriteler ve kuruluşlar da bu düzenlemeleri neredeyse aynen benimsemiştir. COSO (Committee of Sponsoring Organizations) aşağıda belirtilen beş mesleki sivil toplum örgütü tarafından desteklenmekte olup komite, bu kurumlardan tamamıyla bağımsız endüstriden, kamu muhasebesinden, yatırım firmalarından ve New York Borsası'ndan gelen temsilcilerinden oluşmaktadır.

- AICPA: Amerikan Yetki Belgeli Kamu Muhasebecileri Örgütü
- AAA: Amerikan Muhasebe Derneği (muhasebe akademisyenleri/araştırmacıları örgütü)
- FEI: Uluslararası Finansal Yöneticiler Enstitüsü
- IIA: Uluslararası İç Denetçiler Enstitüsü
- IMA: Eski Adıyla Yönetim Muhasebecileri Enstitüsü yeni adıyla Ulusal Muhasebeciler Kurumu (National Association Of Accountants)

COSO, İlk kez 1985 yılında Hileli Finansal Raporlama Ulusal Komisyonu'na destek sağlamak amacıyla kurulmuş bir özel sektör girişimidir. Esas olarak hileli finansal raporlamaya yol açabilen ihmal edilmiş ya da dikkatten kaçan etkenler üzerinde çalışır ve halka açık şirketler, bağımsız denetçiler, Amerikan Sermaye Piyasası Kurulu (SEC) ve diğer düzenleyiciler ile eğitim kurumları için tavsiyeler geliştirir. İlk başkanının adı James C. Treadway olduğu için komisyon bu kişinin adıyla da anılmaktadır. COSO bugün dünyanın her tarafında örgütsel yönetişim ve performansın geliştirilmesi, iç kontroller, kurumsal risk yönetimi, hilenin önlenmesi konularına eleştirel bir bakışla rehberlik sağlayan ve bu konularda düşünce liderliği misyonunu üstlenen bir kurum olarak kabul görmektedir. (Cömert, 2015: 23).

Kuruluşundaki ilk amacı hileli finansal raporlamaya yol açan etkenleri tanımlamak ve bunların adım adım azaltılmasını sağlamak olan COSO, 1992 yılında yayınlamış olduğu "Internal Control-Integrated Framework (İç Kontrol -Bütünleşik Çerçeve) başlıklı raporu ile iç kontrol kavramını irdeleyerek bu konudaki görüş ve önerilerini yayınlamıştır. Söz konusu Çerçeve 2013 yılında bazı değişiklikler yapılarak güncellenmiştir.

COSO İç Kontrol- Bütünleşik Çerçevesinde, iç kontrolü şöyle tanımlamıştır: İç kontrol genelde işletmenin yönetim kurulu, üst yönetimi ve diğer personeli tarafından gerçekleştirilen ve faaliyetlerinin etkili ve verimli olması, raporlamasının güvenilir olması ve ilgili yasalara ve düzenlemelere uygun şekilde çalışılması amaçlarına ulaşılıp ulaşılmadığı konusunda makul ölçüde güvence sağlamak üzere tasarlanan bir süreçtir. COSO'ya göre iç kontrol işletmelerde bu üç temel amacı -faaliyetler, raporlama ve uygunluk- başarmak için tasarlanan şu beş bileşenden oluşur: (COSO, 2013:2-4).

1. Kontrol ortamı,
2. Risk değerlendirme
3. Kontrol aktiviteleri (eylemleri)
4. Bilgi ve İletişim
5. İzleme eylemleri

COSO 2013 güncellenen çerçevesinde bu beş bileşenin birlikte mevcut ve işler durumda olması halinde kontrollerin etkili olabileceğine işaret eder. Bu bileşenlerden birisindeki eksiklik ya da yetersizlik bir riske cevap verememe, önlem alımamış ya da alınan önlemin işe yaramaması anlamına gelir. İç kontrolün bu beş bileşeni güncel Çerçevede ilkeler halinde açıklanmıştır. İyi bir iç kontrol sistemi bu ilkelere uygun şekilde işlemelidir. Hiçbir iç kontrol sistemi doğasında olan bazı kısıtlar sebebiyle mükemmel değildir. İnsanlar tarafından tasarlanır, çoğu insanlar tarafından gerçekleştirilir ve etkili bir şekilde işleyip işlemediği de büyük ölçüde insanlar tarafından izlenir. İnsan unsurunun fazla olduğu (elle işletilen kontrollerin fazla olduğu) işletmelerde kontrollerin ihmali ya da ihlali ihtimali daha yüksektir. Yöneticilerin iç kontrolleri ihmal ve ihlal etme yeteneği her zaman mümkündür. Ayrıca iç kontrollerde fayda-maliyet ilişkisi de diğer bir kısıt unsurudur. İşletmede kontroller oluşturulurken faydanın maliyetten yükek olması beklenir. Ancak faydayı ölçmek maliyeti ölçmek kadar kolay bir iş değildir.

COSO'nun iç kontrol sisteminde amaçlar ve bileşenler arasındaki ilişki üç boyutlu bir küp ile ifade edilmiştir. Bu küpe COSO Kübü denir. (Şekil 3)

Şekil 3. COSO Kübü

Kaynak COSO 2013 Yönetici Özeti

Kübün üst boyutunda işletmenin üç temel grupta ifade edilen amaçları yer almaktadır.

- Faaliyetlere ilişkin amaçlar: Bu amaçlar, faaliyetler ve finansal performans hedefleri ile kayıplara karşı varlıkların korunması da dahil işletmenin faaliyetlerinin etkililiği ve verimliliğiyle ilgilidir.
- Raporlamaya ilişkin amaçlar: Bu amaçlar, iç ve dış finansal ve finansal olmayan raporlamayla ilgili olup güvenilirliği, zamanındalığı ve şeffaflığı veya düzenleyicilerin tanınmış standart koyucuların öngördüğü başka şartları ya da işletmenin politikalarını kapsayabilir.
- Uyuma ilişkin amaçlar: Bu amaçlar, işletmenin tâbi olduğu kanunlara ve düzenlemelere bağlı olmasıyla ilgilidir.

Bu amaçlara uygun şekilde tasarlanan kontroller beş bileşenle ve bu beş bileşen de 17 ilke ile ifade edilmiştir. Hem amaçlar hem de bileşenler (ilkeler) işletmenin tümü, bir bölümü, bir faaliyet birimi **veya** fonksiyonu için oluşturulur ve amaçlara uygun şekilde tasarlanan beş bileşen, birbiriyle bütünleşik ve birlikte işler. Çerçeve, etkili bir iç kontrol sisteminin gerekliliklerini ortaya koyar.

Etkili bir iç kontrol sistemi; bir işletmenin amaçlarının başarılması konusunda makul bir güvence sağlar ve bir işletmenin amaçlarını başaramama riskini kabul edilebilir bir düzeye indirir.

İşletmenin yönetim kurulu ve üst yönetiminin iç kontrollerin makul seviyede tasarlandığına güvenebilmesi için bir iç kontrol sisteminde şu hususlar çok önemlidir:

- Dış olayların, amaçların başarılması üzerinde önemli bir etki yapma ihtimali göz önünde bulundurulduğunda veya işletmenin bu dış olayların niteliği ve zamanlamasını makul bir şekilde öngörebildiği ve etkilerini kabul edilebilir bir düzeye indirebildiği durumlarda etkili ve verimli faaliyetler gerçekleştirilir.
- Dış olayların, amaçların başarılması üzerinde önemli bir etki yapabileceği ya da işletmenin bu dış olayların niteliğini ve zamanlamasını makul ölçüler içerisinde öngörebildiği ve bunların etkilerini kabul edilebilir bir düzeye indirebildiği durumlarda, faaliyetlerin ne oranda etkili ve verimli bir biçimde yönetilebildiği anlaşılır.
- Uygulanabilir kurallara, düzenlemelere ve standartlara ya da kuruluşun belirlediği raporlama amaçlarına uygun olarak raporların hazırlanması.
- Uygulanabilir kanunlara, kurallara, düzenlemelere ve dış standartlara uyulması.

3.1.1. İç Kontrol Sisteminin Bileşenleri ve İlkeleri

COSO'nun önerdiği iç kontrol sisteminin beş bileşeni ve aynı kapsamda 17 ilkesi de aşağıda özlü bir şekilde açıklanmıştır (COSO 2013 Yönetici Özeti)

- Kontrol ortamı
- Risk değerleme
- Kontrol eylemleri
- Bilgi ve iletişim
- İzleme eylemleri

3.1.1.1. Kontrol Ortamı

İç kontrol ortamı, çalışanların görevlerini yapabilecekleri, sorumluluklarını yerine getirebilecekleri ortamı ifade etmektedir. Kontrol ortamı, diğer bileşenler içinde bir temel oluşturmaktadır. Risk değerlendirme, bu değerlendirme için gerekli verilerin toplanması, ilgililere iletilmesi ve bu aşamaların sonucunda izlenip takip edilmesi hep bu ortamda gerçekleştirilmektedir.

Kontrol ortamı, işletmede disiplin ve düzenin sağlanmasına yardımcı olur. Kontrol ortamının unsurları arasında dürüstlük, etik değerler, çalışanların yetkinliği, yönetim kurulu, denetim komitesi, yönetimin çalışma şekli, örgütsel yapı, personel politikaları, yetki ve sorumluluklar yer almaktadır.

Dürüstlük ve etik değerler: İşletmenin hedeflerine ulaşma yöntemleri, işletmenin yönetim şekline ve işletme içindeki değer yargılarına bağlıdır. Bu noktalar, yönetim dürüstlük ve etik değerler hakkındaki düşünce tarzını yansıtmaktadır. İşletmenin itibarının çok kıymetli olması sebebiyle, yasalara uymanın ötesinde davranış kurallarına uymakta bir o kadar önemlidir.

İşletmenin tüm faaliyetlerinde önkoşul etik değerlerdir. İşlemenin iç kontrollerinin oluşturulmasında, yürütülmesinde her zaman etik değerlere önem ve öncelik verilmelidir. İşletmenin etik değerleri oluşturulurken tüm paydaşların (çalışanlar, yöneticiler, müşteriler, tedarikçiler gibi) gözönüne alınması gereklidir. Burada bu paydaşlar arasındaki denge kurulmalıdır.

İyi yönetilen işletmelerde, yönetim kademesi etik kurallara hep riayet etmektedir. Bazı durumlarda karın azalması da göze alınıp gerekli aksiyonların alınması sağlanmalıdır. Örneğin, hatalı mal üretildiğinde satışların düşmesi pahasına da olsa kamuoyuna gerekli açıklamalar yapılmalı, bu konuya yönelik önlemler alınmalıdır.

İşletmelerde etik davranışların yaygınlaşmasının en kolay yolu örnek olmaktır. Bu nedenle, bu boktada yine yöneticilere büyük görevler düşmektedir. Neticede, insanlar bağlı oldukları yöneticiler gözlemler ve ona göre davranış şekilleri oluştururlar.

Yetkinilik: Çalışanlar, görev tanımlarında yer alan işleri yapabilecek yetkinlikte olmalıdırlar. Yetkinilik, kişilerin hem bilgi hem de beceri seviyesini ifade etmektedir. Yetkin çalışanların olduğu işletmelerde bu durumdan kontrol ortamı da olumlu şekilde etkilenir.

Yönetim Kurulu & Denetim Komitesi: İşletmelerde, yönetim kurulu ve denetim komitesinin icradan bağımsız şekilde organizasyonda yer alması ve bu mercilerin yetkin kişilerden oluşmasının kontrol ortamına olumlu etkisi vardır.

Kurumsal yönetim anlayışına göre de işletme yönetiminde bağımsız üyelerin varlığı oldukça kıymetlidir. Bu durumda yönetimde dengenin sağlanmasına da destek olur. Yine denetim komitesi ve yönetim kurulunun iç denetçiler ve bağımsız denetçiler ile iletişimlerinin kalitesi de bu noktada önemlidir.

Yönetimin Çalışma Şekli: Yönetimin çalışma tarzı, işletmenin risklere yönelik alacağı kararları ve işletmenin nasıl yönetildiğini belirler. Bazı işletmeler çok cesur kararlar alabilirken bazıları da daha tutucu bir bakış açısı ile yollarına devam edebilirler. Yönetim çalışma şekline örnek olarak, finansal raporlamaya yönelik tutumları, mali tablo tahminleri veya insan kaynakları konularındaki görüşleri vermek mümkündür.

Örgütsel Yapı: Her işletme kendi ihtiyaçlarına göre bir örgütsel yapı geliştirir. Bazı işletmeler matris organizasyon varken bazılarında da doğrudan raporlama mevcuttur. İşletmenin mevcut örgütsel yapısı, tüm faaliyetlerin hem kontrol hem izlemesini gerçekleştiren mekanizmadır. Örgütsel yapı, işletmelerin büyüklüklerine, faaliyet alanlarına göre de değişiklik gösterebilmektedir.

Yetki ve Sorumluluklar: İşletemelerde operasyonların yürütülebilmesinde yetki ve sorumlulukların belirlenmesi ve çeşitli sınırlandırmaların getirilmesi gerekmektedir. İş tanımlarına ve yapılan işin kritikliğine göre yetkiler düzenlenir. Yetki devirleri, yetkinin nerede başlayıp nerede bittiği bu noktada önemlidir. Günlük operasyonlarda yetkiler çoğunlukla işi yapan kişide de olabilir. Hesap verme sorumluluğu yetki çerçevesindeki bileşenlerden biridir. (Cömert, 2019: 130-136)

3.1.1.2. Risk Değerleme

Risklerin değerlemesinden önce işletme öncelikle hedeflerini belirlemelidir. Sonrasında bu hedeflere ulaşılmasını engelleme ihtimali olan tehditler ve belirsizlikler yani riskler öngörülür ve bu risklere yönelik önlem planları oluşturulur. Riskleri sıfıra indirmek mümkün değildir. Her işletme mutlaka büyüklüğüne, bulunduğu sektöre göre ve işletme içinde her seviyede farklı risklerle karşı karşıyadır. İşletme yöneticileri için önemli olan bu riskleri yönetebilecek belli bir seviyeye indirebilmek ve bu seviyede tutabilmektir.

İşletmeler hedeflerini vizyon ve misyona uygun şekilde belirler. İşletmenin faaliyetler, raporlama ve uyumla ilgili hedefleri iyi planlama yaklaşımıyla kurumsal planlar ve stretejilerle oluşturulur. Stretejik

hedeflerden daha somut spesifik hedefler ortaya konulur. Bu noktada, kaynak planlaması da yapılır. Amaçlar belirlendikten sonra riskler tanımlanır. Nicel, nitel vb bir çok teknikle riskler analiz edilerek etkisi ölçülmeye (tahmin edilmeye) çalışılır. Bu aşamayı takiben, amaçlara uygun şekilde önceliklendirilen riskleri bertaraf edecek veya etkisini azaltacak kontrol eylemleri (aksiyonlar-önlemler) seçilir ve uygulamaya konulur. Önlemler seçilirken kaynaklar en öncelikli risklere tahsis edilir. (Cömert, 2019: 137-145)

3.1.1.3. Kontrol Eylemleri

Kontrol eylemleri, işletmenin faaliyet, finansal raporlama ve uygunluk amaçlarına uygun şekilde üç grupta sınıflandırılır. Örneğin satıcılarla karşılıklı yükümlülük şartlarını belirleyen bir satınalam sözleşmesi yapılması bir faaliyetle ilgili bir kontrol eylemidir. Ancak bir kontrol eylemi bu üç grupla da ilgili olabilir. Faaliyetin etkili ve verimli olması için alınan bir önlem aynı zamanda yasal gerekliliklere uyumu da sağlayan bir kontrol eylemi olabildiği gibi finansal ve finansal olmayan raporların zamanında sunulması amacına hizmet eden bir kontrol eylemi de olabilir. Örneğinin üst yönetime sunulan aylık faaliyet raporlarının izleyen ayın en geç 5 işgünü içinde sunulması kararı faaliyetle ilgili amacın başarılmasına hizmet eden bir önlem olsa da gelir tablosunun da zamanında düzenlenmesi ve vergi dairesine yükümlülüklerin zamanında yerine getirilmesi amacına da hizmet eden bir kontrol eylemidir.

Kontrol eylemlerini çok çeşitli şekillerde sınıflandırmak mümkündür. Örneğin kontrol eylemlerini kontrol amaçları bakımından tespit edici kontroller, önleyici kontroller, düzeltici kontroller şeklinde sınıflandırabiliriz. Kontrol araçları bakımından kontroller, bilgisayarlı kontroller ve manuel(elle işletilen) kontroller şeklinde sınıflandırılabilir. Sistem uzmanları kontrolleri hard (katı) kontroller ve soft (yumuşak) kontroller şeklinde de sınıflandırabilmektedir. Örneğin hergün banka ile düzenli mutabakat yapılması hard kontrol iken, şirkette her kademede çalışanlar tarafından benimsenmiş etik değer ve davranışlar soft kontrol eylemidir.

Kontrol eylemlerine örnek vermek gerekirse; İşletme varlıklarının ve kıymetli evrak ve belgelerin fiziki sayımları ve bunların kayıtlarla karşılaştırılması, üst düzey gözden geçirmeler, karşılaştırmalar, mutabakatlar, onaylar, yetkilendirmeler, görevlerin ayrılığı ilkesinin uygulanması gibi önlemlerin her biri bir kontrol eylemidir. İşletmeler kontrol eylemlerini belirlerken kritik başarı faktörlerine odaklanmalı ve bütçeler, balans skor kartları gibi performans göstergeleri oluşturulmalıdır. Kontrol eylemleri içinde

performans göstergeleri anahtar vazifesi görür. Faaliyetle ilgili olan konular genellikle finansal konularla birleştirilerek değerlendirilir. Her konuya yönelik ilgili performans göstergesi farklı olacaktır. Siparişlerin getiri oranı ya da satın alınan ürünlerin alım fiyatları bu göstergelere örnek olarak verilebilir (Cömert, 2019: 145-151)

3.1.1.4. Bilgi ve İletişim

İşletmeler, iç kontrolün işlevini yerine getirmesini destekleyecek ilgili, nitelikli bilgiyi elde eder veya bu bilgiyi üretir ve kullanır. Aynı kapsamda iç kontrol amaç ve sorumlulukları da dâhil, iç kontrolün işlevini yerine getirmesini desteklemek için gereken bilgileri hem kendi içinde iletir hem de iç kontrolün işlevini yerine getirmesini etkileyen konularla ilgili dış taraflarla iletişim kurar.(COSO Yönetici Özeti 2013)

Kontrollerin diğer bileşenlerinin mevct işler olabilmesi için işletmenin her seviyesinde ihtiyaç duyulan (karara yararlı) bilgilerin işletme içi ve dışından elde edilmesi, işletme içinde işleme tabi tutularak doğru kişilere, doğru zamanda ve doğru ve dürüst bir şekilde iletilmesi gereklidir. Bu bilgiler finansal bilgiler olabildiği gibi finansal olmayan bilgiler de olabilir. Bilgiler, günümüze bilgi sistemleri içinde depolanır, burada işlenir ve ilgili birimlere/kişilere raporlanır. Bilgilerin içeriğinin doğru olması, yetkili kişiler tarafından bilgiye istenildiği zaman ulaşılabiliyor olması ve bilginin güvenli şekilde depolanabilmesi ve bilginin kalitesini belirleyen önemli özelliklerdir.

Faaliyetlerin yürütülebilmesi, raporlama ve uygunluk amaçlarının başarılması için elde edilen doğru bilgilerin, işletme içinde uygun araçlarla (sözlü, yazılı, elektronik, audio, video vb) anlaşılabilir bir şekilde yerinde ve tam zamanında iletilmesi önemlidir.

Gerek kurum içi gerek kurum dışı taraflarla iletişimin zamanında ve verimli sonuçlar doğuracak şekilde yapılabilmesi için, herkesin kendi rol ve sorumluluklarının farkında olması ve bilgiyi doğru aktarabilmesi için birlikte çalıştığı ekibin görevlerine yönelik de bilgi sahibi olması önemlidir.

Bilgi aktarımı konusunda muhataplar sadece işletme içindeki birimler/kişiler değildir. İşletme dışında olan ve işletmenin paydaşı konumunda yer alan herkes bilgilendirilmeye ihtiyaç duymaktadır. Bilgi iletişim alanında, iç denetçiler ve bağımsız denetçiler de ihtiyaçları olan bilgilere kolaylıkla ulaşabilmelidirler. (Cömert, 2019: 151-161)

3.1.1.5. İzleme

İç kontrol adımlarının etkili şekilde gerçekleşmesinde gözlemin (izlemenin) önemli rolü vardır. Gözlem; sürekli izleme veya ayrı ayrı değerlendirmeler şeklinde yapılabilir. Burada önemli olan nokta, bir işletmede sürekli izleme ne kadarı düzenli ve sık yapılıyorsa orada ayrı değerlendirmelere o kadar az ihtiyaç olacaktır. Yine işletmeler, ayrı değerlendirmeleri ne sıklıkta yapmaları gerektiğine karar verirken, olası riskleri, gerçekleşme ihtimallerini göz önüne alırlar.

Sürekli gözlemler gerçek zamanlıdır ve değişen koşullara uyum sağlayarak tekrar düzenlenir. Ayrı değerlendirmeler ise, olay sonrası yapılan faaliyetlerdir. Bu nedenle, sürekli gözlem ile sorunlar daha çabuk tespit edilebilir. Sürekli izleme eylemlerine örnek olarak, zamanında ve doğru raporlama, işletme dışındaki muhataplarla düzenli yapılan mutabakatlar, iç denetim, bağımsız denetim, fiziki sayımlarla kayıtların karşılaştırılması sayılabilir.

Ayrı değerlendirmelere genellikle ayrı bir durumun varlığı halinde ihtiyaç duyurlur. Birleşmeler, bölünmeler, önemli yöneticilerin veya krtik personelin değişmesi, yeni bir ürünün piyasaya sürülmesi veya yurt dışında yeni bir faaliyet birminin açılması gibi durumlarda iç kontrol sistemini ayrı bir değerlendirmeye tabi tutmak ve mevcut önlemlerin yeni risklere cevap verme yeteneğini anlamak gerekir. Sürekli ve ayrı değerlendirmeler çeşitli şekilde yapılabilmektedir. Yöneticilerin düzenli gözetim eylemleri, birim çalışanlarının kendi faaliyetlerini öz değerlendirmeye tabi tutmaları, iç ve dış denetçilerin yaptıkları düzenli veya ani denetimler iç kontrollerin değerlendirilmesine imkan veren durumlardır.

Bu değerlendirmeler, uzman değerlendiriciler tarafından anket, görüşme, kontrol listelerinin hazırlanması, iş akış şemalarının hazırlanması vb gibi biçimsel yöntemlerle gerçekleştirilebileceği gibi iyi uygulamalarla karşılaştırmalar şeklinde de yapılabilir. Özellikle bağımsız denetçiler, işletmelerin iç kontrollerini farklı firmaların iç kontrol sistemleriyle karşılaştırma imkanına sahiptirler. (Cömert, 2019: 161-168)

3.1.2. İç Kontrolün Kurumsal Risk Yönetimi ile Bağlantısı

Kurumsal risk yönetiminin en önemli parçası iç kontroldür. Kurumsal risk yönetimi sistemi iç kontrolü içerir, bu da yönetime daha güçlü fikirler ve kaynaklar sağlamaktadır. İç Kontrol – Bütünleşik Çerçeve, yönetime makul güvence verebilecek bir iç kontrol sistemini açıklamaktadır. İç kontrol için bu yapı, mevcut kurallar ve düzenlemeler için bir rehber oluşturmaktadır. İşletmenin iç kontrol yapısı, kurumsal risk

yönetimi yapısı ile uyumlu tasarlanır. İşletmede hem çalışanların hem de yöneticilerin iç kontrollerin tasarlanması hem de risk yönetiminin tasarlanması süreci içinde yer almaları, işletmede her seviyede farkındalığın artırılması bakımından önemlidir. (Keskin, 2010:45)

İşletmelerin var oluş amaçları ya da temel misyonları, işletmenin sürdürülebilirliğini sağlamak ve bunun bir ölçüde göstergesi olan karını maksimize etmektir. Kar etmeyen şirketler ya da zarar eden şirketler sonuçta batar. Başarılı olmayı tehdit eden riskleri öngörerek tasarlanan iç kontroller, işletmenin misyonunu ve vizyonunu gerçekleştirmesini sağlar. Kurumsal risk yönetimi de işletmenin hedeflerine ulaşmasını tehlikeye sokma potansiyeli olan tüm riskleri ve işletmenin önünü açacak olan tüm fırsatları öngörüp risk yönetimi süreci içinde takip ederek işletmenin vizyon ve misyonu doğrultusunda gitmesine olanak sağlar. (Özer, Erdem 2022:67) Bu bağlamda, bu iki süreç birbiriyle ilişkilidir. Riskler doğru teşhis edilebilsin ki, iç kontrol eylemleri diğer deyişle önlemler (aksiyonlar) işe yarasın. COSO kontrol modelinde bu nedenle risk değerlendirme bileşeni en kritik bileşendir. Sadece kontroller tasarlanırken değil, işletilip ugulanırken ve denetlenirken de riskler sürekli teşhis ve çözümlemeye tabi tutulur.

3.1.3. İç Kontrol ve İç Denetim İlişkisi

IIA'in dünya genelinde kabul gören tanımına göre, iç denetim, bir işletmenin faaliyetlerini geliştirmek ve onlara değer katmak amacını güden; bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetimi, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek işletmenin amaçlarına ulaşmasına yardımcı olur.

Tanımdan da anlaşılacağı üzere, iç denetim fonksiyonel bir görev alanıdır. İç kontrol ise bir süreçtir. İç denetimin temel işlerinden biri, iç kontrollerin gereği gibi tasarlanıp tasarlanmadığını, uygun şekilde uygulanıp uygulanmadığını, kontrol eylemlerinin (önlemlerin) riske cevap verme yeteneğini koruyup korumadığını denetlemektir. Her işletme de iyi ya da kötü iç kontroller vardır. Ama her işletmede iç denetim (teftiş) birimi olacak diye bir zorunluluk yoktur. Küçük işletmelerde üst yönetim ya da sahipler kendi denetimini kendileri yaparlar. Kontrol yönetsel işin bir parçasıdır. Diğer değişle, kontrol yönetimin fonksiyonudur. Bu fonksiyonunu başka birine delege edebilirler. En üst seviyede gözetim ve denetim organı olan yönetim kurulu oluşturduğu iç kontrol sisteminin gözetimi ve denetimi işini denetçilere devredebilir. İşletme içinde bu amaçla oluşturulan denetim birimine iç denetim denir. İç denetim, üst yönetime güvence

verdiği için işletmenin icrai (executive) faaliyetlerinden bağımsız konumda ve tarafsız bir zihniyetle çalışan, yetkili ve ahlaki kodlara bağlı iç denetçilerce yapılırsa güvenilir olur.

Bu açıklamalardan da anlaşılacağı üzere, esasen iç denetimin kendisi de bir iç kontrol eylemidir. İşletmeler büyüdükçe süreçler daha karmaşık hale geldiği için iç denetim fonksiyonuna olan ihtiyaç da artar. İç denetçiler kontrollerin tasarımında rol almamalıdır. Kendi tasarladıkları kontrolleri denetlemeleri bağımsızlıklarına ve tarafsızlıklarına zarar verir. İç kontrollerle ilgili bazı danışmanlık hizmetleri verebilseler de bu hususa özen göstermeleri gerekir.

3.2. Kurumsal Risk Yönetimi Genel Çerçevesi ve Önemi

Risklerin tek başına ve birbirlerinden bağımsız şekilde yönetilmeye çalışılmasının işletmeler için ciddi zorlukları olduğu zaman içinde anlaşılmıştır. Yaşanan sıkıntılardan yola çıkılarak oluşturulan kurumsal risk yönetimi kavramında ise tüm olası risklerin bir bütün olarak detaylı bir şekilde değerlendirilmesi, birbirleriyle olan ilişkilerinin ve birbirlerine olan etkilerinin ortaya konması amaçlanmaktadır.

Kurumsal risk yönetimi, işletme bünyesinde oluşturulan yapılandırılmış, düzenli ve tutarlı bir sistemdir. Bu system, hem risklerin hem de fırsatların belirlenmesi, değerlendirilmesi, risk cevaplarının oluşturulması ve raporlanmasına yönelik süreci içerir. (Pickett, 2005:4)

Kurumsal risk yönetimi, kurumun hedeflerine ulaşmasını etkileyen fırsatların ve tehditlerin tespit edilmesi, tanımlanması, değerlendirilmesi, bunlara verilecek yanıtların kararlaştırılması ve bunların rapor edilmesi için tüm kurum çapında uygulanan, özel yapılandırılmış, istikrarlı, tutarlı ve devam eden bir süreçtir.

Kurumsal risk yönetiminin en belirgin özellikleri aşağıda sıralanmıştır: (Saka, Uğural, 2008:16)

- İşletmelerde durağan veya bir kere gerçekleştirilen bir süreç değil devamlılığı olan bir süreçtir.
- Amacı, sadece olası tehditleri bertaraf etmek değil aynı zamanda da gelir yaratmak ve katma değer oluşturmaktır.
- Bölüm/kısım bazında değil işletmenin her biriminde aynı zamanda ve aynı şekilde uygulanır.
- Yapılan tüm çalışmalarda işletmenin risk iştahı dikkate alınır.
- Üst düzey yöneticilerin stratejileri belirlerken göz önüne almaları gereken en önemli noktalardan biri KRY'dir.

- İşletmenin sürekliliğinin sağlanmasındaki en önemli sistemlerden birisi olan erken uyarı sisteminin temelinde yer alır.
- Kurumsal risk yönetimi, iç kontrolü kapsayıcı niteliktedir.
- Kaynakların etkili olarak dağıtılması, operasyon planları ve diğer yönetim araçları ile beraber değerlendirilir.
- Risklerin en aza indirilmesini hedeflerken aynı zamanda da operasyonun sürdürülebilirliği açısından riskten kaçınmak sorun teşkil ediyorsa işletmenin risk iştahı göz önünde bulundurularak ilgili riskin alınmasını tavsiye eder.
- Risklerin süreçler üzerindeki domino etkisinin ortaya çıkarılmasında etkili rol oynar.
- İşletme içi verimliliğinin artırılmasını ve standartların korunmasını garanti altına alır.
- Sadece riskler üzerine yoğunlaşmaz. Aynı zamanda olası fırsatların tespit edilmesi, ölçülmesi, takip edilmesi safhasında da üzerine düşen görevleri yapar.

Yukarıdaki özelliklerden de anlaşılacağı üzere, kurumsal risk yönetimi yapılandırılmış organizasyonel bir süreçtir. Bu yapısı ve olaylara hem bütünsel hem de sistematik yaklaşması ile organizasyon için risklere yönelik farkındalığın artmasını ilk hedefine koymaktadır. Eğer bir organizasyonun her seviyesinde olası tehditlere yönelik farkındalık gelişirse, süreci en az hata ile uygulamak ancak o zaman mümkün olur.

Kurumsal risk yönetimi çerçevesi mutlaka işletmenin yönetim sisteminde stratejik planlama, karar alma sistemleri ve risklerin ortaya çıkarılmasına yönelik diğer tüm stratejilerin, süreçlerin var olmasını gerektirmektedir. (Pickett, 2005:27)

Kurumsal risk yönetiminin işletmelerde etkili bir şekilde gerçekleştirilebilmesindeki en önemli etkenlerden biri kontrol ortamının kaliteli olmasıdır. Olması gereken kontrol ortamının tarifi aşağıdaki gibidir: BU TARİF NEREDEN GELMİŞ COSO iç kontrolden geliyorsa alt bileşenler eksik

Yönetimin Yaklaşımı Yönetimin performans temelli bir yaklaşımı benimsemesi, risk yönetimi sistemini işletme içinde etkili uygulamaya çalışması, kurumsal risk yönetiminin adımlarına karşı saygılı ve sağduyulu hareket etmesi, şirket içi süreçlerde güvenilir bilgi-işlem ve personel sistemlerinin kullanılması doğru kontrol ortamının oluşmasına önemli katkı sağlamaktadır.

Dürüstlük ve Etik Değerler: İşletmenin tüm kararlarında ve uygulamalarında temelde yer alması gereken kavram dürüstlüktür. Başta yöneticiler olmak üzere tüm personel dürüst davranmak zorundadır.

Çalışanlardan bu konudaki beklentiler net şekilde açıklanmalı ve bu beklentiler karşılanmadığında gerçekleşecek yaptırımlarda anlatılmalıdır. Bu süreç yürürken yöneticilerin tüm çalışanlara davranışlarıyla örnek teşkil etmeleri de beklenir. Birçok işletmede etik kod olarak da ifade edilen çalışmalarda da detayları anlatılan etik davranışlara uygun kurum kültürünün oluşturulmasında etkili iç denetim fonksiyonunun varlığı, personelin bireysel performansını objektif ölçen bir performans yönetimi sisteminin mevcut olması ve üst yönetim aracılığıyla bu konuya ilişkin farkındalığın yaratılması önemli rol oynamaktadır. (Tekgül 2007:4)

Organizasyonel Yapı: İyi planlanmış bir organizasyon yapısı, yöneticilerin karar alma sürecinde yardım almalarını, hızlı kararlar almalarını ve gerekli bilgiye hızlı erişebilmelerini sağlamaktadır. İşletmelerin organizasyonlarının nasıl olması gerektiği belirlenirken, işletmelerin çeşitli özellikleri göz önünde bulundurulmalıdır. Bulundukları sektör, çalışma alanları, çalışma biçimleri, büyüklükleri, pazardaki yerleri vb. dikkate alınmalıdır. Tabii ki işletmenin misyonu ve vizyonu da bu noktada etkilidir. Misyon, işletmenin varoluş amacını ifade ederken vizyon, işletmenin gelecekte ne yapmak istediğini göstermektedir. Şirket hedefleri, vizyon ve misyonu belirler. Bu belirleme aşamasının ardından, bu vizyon ve misyona uygun olarak çalışacak olan yapıyı oluşturma aşaması gelmektedir. Bu yapı, duruma göre matris, hiyerarşik veya fonksiyonel olabilmektedir.

Kurumsal risk yönetiminin en önemli hedeflerinden, işletmelere "risk zekası" kavramını benimsetmektir. Risk zekasına sahip işletmeler de, risk yönetimi uygulamaları tüm işletmeye yayılmıştır. Bu işletmelerin faaliyet gösterdikleri sektörlerde risk yönetimi süreci aynı titizlikle uygulanmaktadır. Risk çeşitlerinin tamamı (operasyonel, stratejik, mevzuat, olağanüstü riskler vb.) bu süreç içinde dikkatli şekilde takip edilmektedir. Risk zekası gelişmiş olan işletmelerde, kurumsal risk yönetiminin bir sonucu olarakta riskler ayrı ayrı değerlendirilmez, birbiriyle ilişkili riskler birarada değerlendirilir ve bütünleşik senaryolar üretilir. Bu işletmelerde risklerden kaçınmaktan ziyade riskleri makul seviyede kabul ederek uygun önlemleri alarak operasyonun güvenliği ve sürekliliği sağlanmaktadır. (Tekgül 2007:4)

Kurumsal risk yönetimi çerçevesinin temel kavramlarından biri de yukarıdaki bölümlerde de anlatılan risk kültürüdür. Risk kültürü denildiğinde bir işletmede riskin karşılanma şekli, riskin anlaşılması ve değerlendirmesine yönelik davranışların bütünü ve risk sistemleri-süreçleri boyunca organizasyonların içinde yer alan tüm bireylerin takındıkları tutumlar ve davranışları anlaşılmaktadır. Bir işletmenin başarılı olması için risk kültürünün işletmenin her seviyesindeki çalışanları/yöneticileri tarafından benimsenmiş

olması gerekir. Bu süreçte işletmenin alabileceği risklerin büyüklüğü ve uygulayacağı risk stratejileri bu kavram ile çok ilintilidir. Riskler karşısında bilinçli davranılmalı, risk değerleme bağımsız bir ortamda yapılmalı, riskleri azaltan faktörler üzerine yoğunlaşılmalıdır. Risk kültürü, işletmelerde negatif değil pozitif ve bir adım daha öteye gidildiğinde proaktif bir yaklaşıma dayalı olmalıdır. (Fikirkoca, 2003: 46-47)

İşletmelerde kurumsal risk yönetimi sürecinin uygulanması, riskleri azaltmakla birlikte risklerin daha iyi nasıl taşınabileceğini de işletmeye öğretmektedir. (Glowka, 2020:1216).

Kurumsal risk yönetiminin uygulamaya alınmasında birçok uluslararası standart ve çerçeve etkili olmuştur. Öncelikle özel sektörde faaliyet gösteren işletmeler tarafından bu çerçeve ve yasal düzenlemeler kabul görmüş ve uygulanmaya başlanmıştır. Genelde ikinci planda olduğu düşünülse de, kamu sektöründe de zamanla kamu işletmeleri ile ilgili olan kişilerin/kurumların talepleri, bu alanda da uluslararası düzenlemelere uyma ihtiyacı, kamu yönetimi anlayışındaki farklılaşmalar, şeffaf bilgi paylaşımı ve şeffaf yönetim düşüncesinin kamu idarelerinde önem kazanması gibi nedenler ile kurumsal risk yönetimi konusu kamu alanında da görüşülen bir gündem konusu haline gelmiştir. (Ilgar, Erdoğdu 2018: 64) Tüm bu gelişmeler kamu veya özel her işletmenin kurumsal risk yönetimi konusunda kendisini geliştirmesini ve aksiyon almasını gerekli kılmıştır.

Kurumsal risk yönetiminin başarıya ulaşması için yönetim kurulu ve üst düzey yöneticiler tarafından tam kabul görmüş olması ve bu kişilerin sistemin uygulanması aşamasında rol model olarak yer alması gerekir. Aksi takdirde, işletmelerde kurumsal risk yönetiminin işletmenin sürdürülebilirliğine katkı sağlaması, karar alma mekanizmalarını aydınlatması, işletmenin hedeflerine ulaşabilmesi için yapılması/yapılmaması gerekenleri ortaya koyması beklenemez.

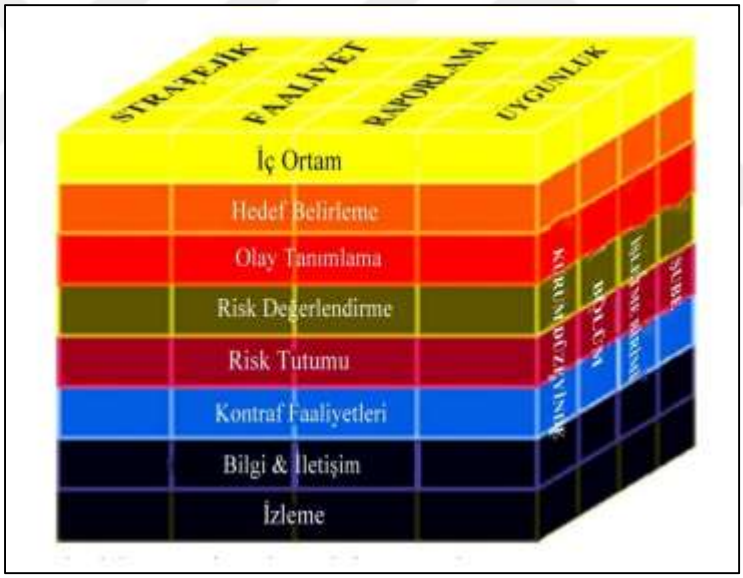
3.2.1. Kurumsal Risk Yönetimi Modelleri

3.2.1.1. COSO

İç kontrol modelleri içinde en çok kabul gören COSO'nun (Committee of Sponsoring Organizations of the Treadway Commission) Bütünleşik Çerçeve veya İç Kontrol Entegre Çerçevesi ismiyle 1992'de yayımladığı çalışmasıdır. Bu çalışma 2013 yılında revize edilmiştir. COSO; Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants), İç Denetçiler Enstitüsü

(Insittute of Internal Auditors), Finansal Yöneticiler Enstitüsü (Financial Executives International), Amerikan Muhasebe Birliği (American Accounting Association) ve Yönetim Muhasebecileri Enstitüsü (Institute of Management Accountants) tarafından kurulmuştur. Kuruluş gayesi ise mali raporlamanın daha kaliteli hale gelebilmesi için etkili iç kontrol ve kurumsal yönetim yapısının oluşturulmasıdır. Diğer çalışma ise 2004 yılında yayınlanan Kurumsal Risk Yönetimi Entegre Çerçevesidir.

2004 yılındaki bu çalışmanın bir özeti aşağıdaki küp şeklinde görülmektedir. Bu küpte sekiz adet bileşen mevcuttur. Bu bileşenler, iç ortam, hedef oluşturma, olay belirleme, risk değerlendirme, kontrol aktiviteleri, bilgi & iletişim ve izlemedir. Kübün yan tarafında ise işletmenin amaçları, yapısı ve kurumsal yönetimin bileşenleri yer alır. (Burca 2017)



Şekil 4: COSO Kurumsal Risk Yönetimi Küpü (2004)

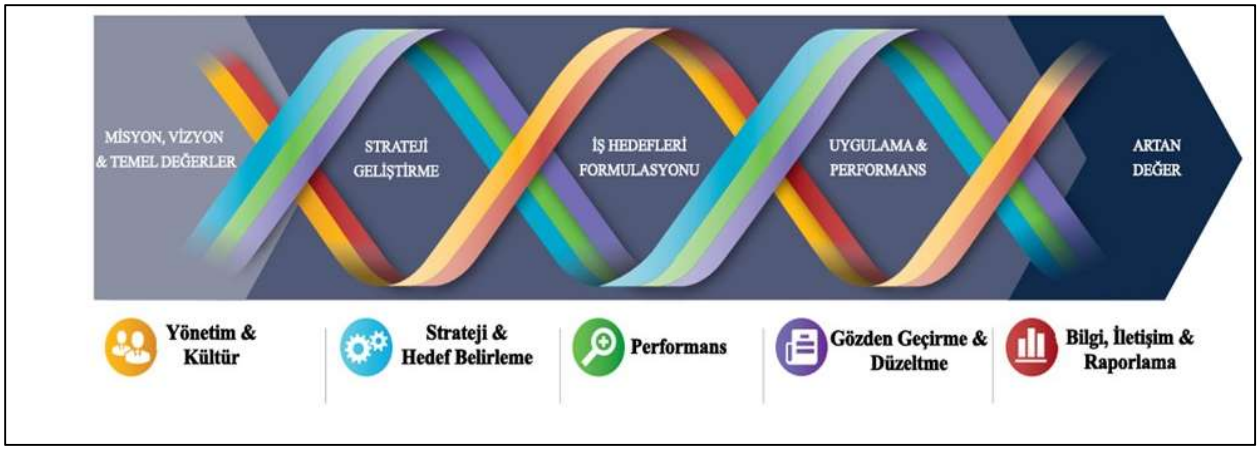
Kaynak: COSO 2004 Kurumsal Risk Yönetimi Çerçevesi

COSO'nun 2004 yılında yayınladığı kurumsal risk yönetimi çerçevesi, günümüzde işletmelerin uyguladığı risk yönetimi süreçlerinin bel kemiğini oluşturmaktadır. Yıllar içinde iş hayatının değişen dinamikleri, teknolojik gelişmeler, işletmelerdeki operasyon çeşitliliği vb etkenler sebebiyle kurumsal risk yönetimi

çerçevesinin güncellenmesinin gerekliliği ortaya çıkmıştır. Bu nedenle COSO, 2014 yılında bu çerçeveyi güncellemiştir. Daha sonra yine oluşan farklı ihtiyaçlara istinaden, 2017'de tekrar bir güncelleme yayınlamıştır. "Riskin Strateji ve Performansla Uyumlaştırılması" adıyla yayınlanan bu güncellemeyi müteakip olarak işletmelerde kendi iç yönetmeliklerini/yönergelerini değiştirmişler ve yeni düzene göre operasyonlarına şekil vermiştir. 2017 yılında yayınlanan çerçevede sürdürülebilir performans, stratejik hedeflerin oluşturulması ve dolayısıyla stratejik planlama konuları gündeme gelmiştir.

COSO 2017'de yenilediği kurumsal risk yönetimi çerçevesi ile günümüz çalışma dünyasına sarmal bir yapı aracılığıyla risk yönetiminin en temeline yönetişim ve kültür kavramlarını koymuştur. Sarmalın asıl gövdesini; strateji ve hedef belirleme (işletmenin hedeflerinin/amaçlarının risk iştahı ile ve stratejileriyle uyumlu şekilde kurgulanması, işletmenin her seviyesindeki risklerinin ve fırsatlarının dikkate alınması), performans ölçümü (risklerin tanımlanması, riskin şiddetinin ölçülmesi, risklerin önceliklendirilmesi ve tüm bunlara bağlı olarak risk yanıtlarıyla portföy bakış açısının oluşturulması), gözden geçirme ve revizyon (işletmenin çalışma hayatı içinde ortaya çıkan değişikliklere göre hedeflerini güncellemesi, bunlar ışığında performansını nasıl sonuçlandırdığı, kurumsal risk yönetim uygulamalarının etkili çalışıp çalışmadığı, kuruma ne kadar değer kattığı ve bu katma değerin işletme açısından sürekli olup olmaması) meydana getirmektedir. COSO Kurumsal Risk Yönetimi sürecinin yan dallarını ise bilgi, iletişim ve raporlama oluşturmuştur. Bu yan dallar sayesinde de, işletme kendi içinden ve dışarıdan bilgiler elde edip, kendi bünyesinde gerekli bilgi paylaşımını yapmalıdır. Sözkonusu bilgiler işletmenin tüm faaliyetlerinde kullanılmakta, işlenmekte ve bu veriler bir süreç mantığıyla işletilmektedir. Sonuç olarak, işletmeler yönetişim, risk, kültür ve performansa ait raporlamalar yapmakta ve bunu ilgililerle paylaşmaktadır. Bu noktada risk envanterinin hazırlanması da büyük önem arz etmektedir. (Güler, Arkın 2019: 98)

Yukarıda gösterilen ve COSO 2004'te yer alan küp yerini 2017'de aşağıda görülen kurumsal risk yönetimi sarmalına bırakmıştır. Sarmal şeklinde ifade edilmesindeki temel amaç, tüm süreçlerin birbiriyle olan iç içe ilişkisinin daha kolay ifade edilmesidir.



Şekil 5. COSO Kurumsal Risk Yönetimi Sarmalı (2017)

Kaynak: COSO Kurumsal Risk Yönetimi Çerçevesi 2017

Bu sarmalda 5 ana bölüm ve bu bölümlerin altında da 20 adet ilke yer almaktadır. Bu beş ana bölümün üç tanesi (2., 3. ve 4.bölüm) işletmede yürütülen süreçleri gösterirken, diğer iki tanesi (1. ve 5. Bölüm) kurumsal risk yönetiminin destekleyici unsurlarını ifade etmektedir.

Bu yeni yaklaşım, kurumsal risk yönetiminin misyon, vizyon ve temel ilkeleriyle nasıl ilişkili olduğunu göstermektedir. Diyagramın üç şeridi (Strateji & Hedef Oluşturma, Perfomans, Gözden Geçirme & Düzeltme) işletmenin genel süreçlerini temsil ederken, diğer iki şerit (Yönetişim & Kültür ve Bilgi, İletişim & Raporlama) kurumsal risk yönetimini desteklemektedir.

Bu sarmalda, kurumsal risk yönetiminin strateji geliştirme, iş hedeflerinin oluşturulması, takip edilmesi ve performans yönetimiyle birleştirilmesinde işletmenin değerinin artacağı varsayımından hareket etmektedir. Kurumsal risk yönetimi dinamik bir oluşumdur ve alınan günlük kararlar aracılığıyla yürütülmektedir. (Burca, 2017).

Son 20 yılda iş hayatında yaşanan gelişmeler, dünya ekonomisinde yaşanan değişimler ve zorluklar kurumsal risk yönetimi sürecine bakışı da farklı bir noktaya taşımıştır. Artık işletmelerde risk farkındalığının oluşması, hedef belirleme aşamasında risk yönetiminin bu adımlara dahil edilmesi ve performans ölçümleme sırasında risk yönetimi çıktılarının kullanılması elzem hale gelmiştir. Bu ihtiyaçlarda COSO'nun 2017 yılında yayınlanan çerçeveyi güncellemesi sonucunu doğurmuştur. Yeni

çerçeve; işletmelerin iş yaşamının günden güne fazlasıyla değişen dinamik şartlarına, iş süreçlerinde ortaya çıkan kompleks yapılara ve aynı zamanda tüm dünyada her alanda görülen hızlı değişimlere daha kolay adapte olmasına aracılık etmektedir. Yeni çerçeve de stratejik karar alma mekanizmalarından yüksek performansa giden yol ifade edilmeye çalışılmıştır. İşletmeler, piyasada rekabet avantajını korumak için atacakları adımlarda kurumsal risk yönetimi adımlarını kullanmaya başlamıştır. Bu şekilde üst yönetimler, işletmelerin stratejilerini belirlerken hangi risklerin nelere yol açabileceği, verebileceği olası zararları daha kolay görebilmektedirler.

COSO 2017 kurumsal risk yönetimi çerçevesinde, bütünleşik risk yönetiminin bir işletmede tahsis edilmesi için stratejik planlama süreçlerinin ne kadar önemli olduğu ve risk yönetiminin stratejik planlama aktivitelerinin bir parçası olması gerektiği vurgulanmıştır. Güncel düzenlemede üzerinde durulan diğer iki kavram da "performans" ve "bütüncül strateji"dir. Bu vurgunun sebebi de, risk yönetimi uygulamalarının işletmelerin hedeflerine ulaşması yolunda aktif rol oynadığının ortaya konulmasıdır. (Pierce & Goldstein, 2018: 52).

Yeni çerçeve ile yönetişim ve işletme içi kültür, strateji ve hedef belirleme, stratejik planlama, şirketin performansının yükseltilmesi ve takibi, hissedarlar ve tüm kamu nezdinde şeffaf ve zamanında bilgilendirmenin yapılması çok ciddi önem kazanmıştır. (Karakaya, G. 2018: 16-18)

COSO 2017'ye göre KRY faaliyetleri bir özet olarak aşağıda sıralanmıştır: (Florea ve Florea 2016: 76- 77):

- İşletmenin hedeflerinin ortaya konması.
- İşletmenin risk iştahının belirlenmesi.
- İşletme içinde uygun bir ortamın (Risk yönetimi çerçevesi dâhil) meydana getirilmesi.
- İşletmenin hedeflerini gerçekleştirmesini tehlikeye sokacak olası olayların belirlenmesi.
- Riskin vereceği hasarın ve gerçekleşme olasılığının ortaya konması.
- Risklere verilebilecek yanıtların seçilmesi ve uygulanması.
- Sürece yönelik kontrol aktivitelerinin organizasyonu.
- İşletmede her seviyedeki çalışanın risklere/fırsatlara yönelik bilgilendirilmesi.

COSO 2017'nin sürece getirdiği katma değeri de aşağıdaki noktalar ile ifade edebiliriz: : (Florea ve Florea 2016: 76- 77)

- İşletmenin stratejilerinin belirlenmesinde risk yönetimi ışık tutan bir rol oynar.
- İşletmenin performansının artırılması yolunda risk yönetimi belirleyici durumdadır. Performans kriterleri arasında kar maksimizasyonu kadar verimlilik gibi belirteçlerde yer alır.
- İşletmeye yönelik gözetim ve yönetişim ihtiyaçlarını daha iyi karşılayacak bir ortam sunar.
- İşletmelerin içinde bulundukları global iş dünyasının ve ait oldukları sektörlerin gerekliliklerini ve standartlarını kabul eder. Aynı zamanda da işletmelere özgü çözümlerin üretilmesine de imkan tanır.
- İşletmenin hedeflerini belirleme ve bu hedeflere ulaşma yolunda karşısına çıkabilecek riskleri daha kolay tayin edebilmesine olanak sağlar.
- Hissedarlara daha şeffaf bilgi paylaşımında bulunulacak ortam yaratılır.
- İşletme üst yönetiminin karar alma süreçlerinin yeni teknolojik gelişmeler ve veri analitiği sistemleri ile desteklenmesi sağlanır.
- Kurumsal risk yönetimi sisteminin tasarlanması, adımlarının belirlenmesi, uygulanması için gerekli tüm bileşenleri belirler.

Kurumsal risk yönetimi zamanla işletmenin karşı karşıya kaldığı farklı durumlar karşısındaki dayanıklılığının artırılmasını da hedeflemektedir. Ayrıca sadece risklerin belirlenmesini değil aynı zamanda süreçlerde gerçekleştirilmesi gereken tüm değişiklikleri, bu değişikliklerin stratejilere ve hedeflere etkilerini de gösterilmesi bu kapsamda yer almaktadır. COSO 2017 ile aşağıdaki beklentiler karşılanmaktadır:

- Risk yönetimi konusu tek başına yürütülen bir alan olmaktan çıkmış ve stratejik planlama, hedef belirleme süreci içine entegre edilmiştir.
- İşletmelerin riskleri daha kolay tahmin etmeleri, risklerin hedefleri üzerindeki etkilerini görmeleri sağlanmıştır.
- Sadece riskleri yönetmek değil aynı zamanda fırsatları da takip etmek, gözden geçirmek ve bu sürece dahil etmek mümkün olmuştur.
- İşletmeler hedeflerini belirleme, o hedeflere giderken yollarına çıkabilecek zorlukları ve aynı zamanda ek başarı ve performans getirecek fırsatları görebilme yolunda kurumsal risk yönetimini etkili şekilde kullanmalıdır.

Stratejik planlama sürecine entegre edilen kurumsal risk yönetimi süreci ile, işletmenin stratejilerini, hedeflerini tehlikeye sokacak riskler önceden tanımlanabilir, buna yönelik önlem planları yapılabilir. Böylece yüksek risk barındırdığı ortaya çıkan stratejilerden, amaçlardan vazgeçilebilmektedir. (Ermisket 2016:56) Bu noktada sadece riskler üzerinden gidilmemeli, fırsatlarda düşünülüp onların çoğaltılmasına ve tespit edilen fırsatlardan elde edilecek potansiyel faydanın artırılmasına yönelikte çalışmalar yapılmalıdır.

COSO 2017 ile şirkette değer yaratma, risk yönetimini işletmenin süreçlerinin içine dahil etme, strateji oluşturma, vizyon ve misyon konularını doğrudan risk yönetimi ile beraber değerlendirme gibi yeni bakış açıları sunmakta ve bu bakış açıları ile kurumsal yönetime de bir yenilik getirmektedir.

COSO 2017'nin COSO 2004'e göre getirdiği farklılıklardan bazıları da teknolojik gelişmelere karşılık işletmelerin göstermesi gereken gelişimler ve tüm yönetim süreçlerinde kurumsal risk yönetiminin günden güne artan rolünün daha iyi anlatılması da yer almaktadır.(Prewett & Terry, 2018:17).

COSO 2017 çerçevesinde işleyen kurumsal risk yönetimi süreçleri, işletmelerin riskleri doğru ve çabuk tanılamasına, oluşabilecek hasarları belirlemesine, sürprizlerin azaltılmasına, doğru öngörüler ile maliyet tasarrufu yapabilmesine, işletmenin faydasına olacak konu-olayların tespitine imkan sağlamaktadır.

2004 düzenlemesiyle karşılaştırıldığında, bileşenlerin altındaki ilkelerin belirlenmesi, çerçevenin anlaşılması daha kolaylaşmıştır denilebilir.

Aşağıda COSO 2004 ile COSO 2017 arasındaki farklılıkları bir özet tabloda yer almaktadır:

Tablo 6. COSO 2004 ile 2017 Kurumsal Risk Yönetimi Çerçevelerinin Karşılaştırılması

COSO 2004 Çerçevesinin Unsurları	COSO 2017 Çerçevesinin Unsurları	COSO 2017 Prensipleri
İç Ortam	**Yönetişim ve Kültür**	Yönetim kurulu, risk gözetimi görevinin yerine getirmesi
		Operasyonel yapının oluşturulması
		Beklenen işletme kültürünün tanımlanması
		İşletmenin temel değerlerine bağlılık gösterilmesi
		Yetenekli çalışanların işletmede istihdam edilmesi, geliştirilmesi ve işletmede uzun süre tutulması
Hedef Belirleme	**Strateji ve Hedef Belirleme**	İş ortamının incelenmesi
		Risk iştahının belirlenmesi
		Olası tüm stratejilerin değerlendirilmesi
		İşletme hedeflerinin belirlenmesi
Olay/Olgu Tanımlama **Risk Değerlendirme** **Riske Karşılık Verme/Kontrol Faaliyet**	**Performans**	Risklerin Belirlenmesi
		Risklerin şiddetlerinin tespit edilmesi
		Risklerin önceliklendirilmesi
		Risklere verilecek cevapların ortaya konulması
		Bütüncül bakış açısının işletmeye yerleştirilmesi
İzleme	**Gözden Geçirme & Revizyon**	Önemli değişikliklerin değerlendirilmesi
		Risk ve ona yönelik performansın gözden geçirilmesi
		Kurumsal risk yönetimi sürecinde iyileştirmelerin takip edilmesi
Bilgi ve İletişim	**Bilgi, İletişim ve Raporlama**	Bilgi ve teknolojideki gelişmelerden faydalanılması
		Riske yönelik tüm iletişimin sağlanması
		İşletmedeki mevcut riskler, risk kültürü ve sürece yönelik gerekli tüm bilgilerin raporlanması

Kaynak: Yazar tarafından oluşturulmuştur.

2017 çerçevesinde, kurumsal risk yönetiminin tanımı bile farklı hale gelmiş ve işletmenin değer yaratma, yaratılan değeri koruma, gerçekleştirme, riski doğru yönetmek için makul stratejileri belirleme ve takip etme noktalarını içeren kültür ve uygulamaları kapsar hale gelmiştir.

Burada önemli olan işletmenin tüm süreçlerinin içine kurumsal risk yönetiminin entegre edilmesidir. Dolayısıyla işletmelerde tek bir birimin değil tüm birimlerin bu konuda risk farkındalığının olması ve bu konuda sürekli düşünüyor ve çalışıyor olmaları gerekir. Yukarıda da yer alan sarmaldaki bileşenler ve prensipler aşağıda açıklanmıştır:

Yönetişim ve Kültür: Bu bileşen, sarmalın en temelini oluşturan kısımdır. Yönetişim, işletmenin kendine özgü yönetim anlayışının tesis edilmesini ifade etmektedir. Burada işletme içindeki tüm roller ve sorumluluklar, görev dağılımları yer almaktadır. İşletmede risk kültürünün oluşturulması, risk

farkındalığının yaratılması da bu bileşenin kapsamındadır. Risk kültürü içinde, etik değerler, çalışanlardan/yöneticilerden beklenen davranışlar, risk anlayışı mevcuttur.(COSO, 2017:6-7).

Bu bileşene ait ilkeler aşağıda yer almaktadır:

a. Yönetim kurulunun risk gözetimi görevinin yerine getirmesi
b. Operasyonel yapının oluşturulması
c. Beklenen işletme kültürünün tanımlanması
d. İşletmenin temel değerlerine bağlılık gösterilmesi
e. Yetenekli çalışanların işletmede istihdam edilmesi, geliştirilmesi ve işletmede uzun süre tutulması

Yukarıdaki ilkeler neticesinde, işletmede yönetim kurulu üyeleri kurumsal yönetim anlayışının işletmede hakim olmasından, hedeflere ulaşmayı sağlamak amacıyla gerekli risk gözetimini yerine getirmekten, risklerin belirlenmesi/değerlendirilmesi aşamalarını gerçekleştirecek olan ve aynı zaman işletmenin hedeflerine ulaşmasını sağlayacak tüm süreçlerin nasıl işleyeceğini belirlemekten sorumludur. Bu noktada yine roller ve sorumluluklarda takip edilmelidir. İşletmenin değerlerine bağlılığın organizasyonun her aşamasına yerleştirilmesi de bu kapsamda gerçekleştirilmesi gereken önemli bir husustur. (COSO, 2017:10) İşletmelerin en kıymetli kaynağı iş gücüdür. Bu kabul ile, doğru kişilerin doğru pozisyonlarda istihdam edilmesi, işletme içinde gerekli eğitimlere tabii tutularak gelişimlerinin sağlanması ve sadakatle çalışabilmeleri için uygun ortamın yaratılması bu bileşenin son ilkesidir.

Strateji/Hedef Belirleme: Bu bileşenin içeriğinde, kurumsal risk yönetimi sürecinin işletmenin hedef belirleme, vizyon-misyon belirleme süreçlerinin içine entegre edilmesi yer almaktadır. Bileşenle ilgili prensipleri aşağıda görebiliriz:

a. İş ortamının incelenmesi
b. Risk iştahının belirlenmesi
c. Olası tüm stratejilerin değerlendirilmesi
d. İşletme hedeflerinin belirlenmesi

İşletmelerin gerçekçi hedefler belirlemeleri organizasyon içinde bu hedeflerin algılanıp peşinden gidilebilme ihtmalini artırmaktadır. Ancak bu şekilde hem işletme içindeki stres yükü hem de aynı zaman da hatalı raporlama ihtimali azalmaktadır. (Pickett, 2005:24)

İş ortamı ile işletmelerin içinde bulunduğu ve etkileşim içinde oldukları dinamik bir alan kastedilmektedir. Pazar şartlarının değişmesi, rakiplerin farklılaşması, ürün gamında olabilecek değişiklikler, teknolojik gelişmeler gibi birçok etken, bu çalışma alanının temel faktörleridir. (Karakaya 2018:19) Tüm bu değişkenler sonucunda işletmenin risklerinde farklılaşmalar olabilir, bu değişikliklere göre işletmenin stratejilerinin de hedefler göz önüne alınarak güncellenmesi gerekir.

Performans: İşletmenin devamlılığını sürdürmesini tehlikeye atacak tüm riskler bu alanda belirlenmekte, değerlenmekte ve takip edilmektedir. Performansın adımları aşağıda yer almaktadır:

a. Risklerin belirlenmesi
b. Risklerin şiddetlerinin tespit edilmesi
c. Risklerin önceliklendirilmesi
d. Risklere verilecek cevapların ortaya konulması
e. Bütüncül bakış açısının işletmeye yerleştirilmesi

Kurumsal risk yönetimi sürecinin her adımı bu alanda yerini alır. Riskler belirlenir, şiddetleri, gerçekleşme olasılıkları belirlenir, riskler önceliklendirilir, risklere verilebilecek cevaplar netleştirilir.

Gözden Geçirme&Revizyon: Kurumsal risk yönetimi uygulamalarının düzenli takibi, eksiklerin giderilmesi, hedeflere ulaşma yolunda ek olarak gerçekleştirilmesi gereken noktaların belirlenmesi bu prensip altında ifade edilmektedir. Bu noktalara giden yolun adımları yani bu bileşenin ilkelerini aşağıda görebiliriz:

a. Önemli değişikliklerin değerlendirilmesi
b. Risklerin ve ona yönelik performansın gözden geçirilmesi
c. Kurumsal risk yönetimi sürecinde iyileştirmelerin takip edilmesi

İşletmelerin stratejilerinde, hedeflerinde olabilecek önemli değişikliklerin öngörülmesi, bunların kurumsal risk yönetimi sürecine etkisi ve bu etkilerin işletme yönetimine ve alınacak kararlara destek olması bu bileşende yer almaktadır.

Bilgi, İletişim ve Raporlama: Kurumsal risk yönetimiyle ilgili düzenli tüm raporlamalar ve oluşturulması gereken çıktılar bu kapsamdadır. Adımları da aşağıda yer almaktadır:

a. Bilgi ve teknolojideki gelişmelerden faydalanılması
b. Riske yönelik tüm iletişimin sağlanması
c. İşletmedeki mevcut riskler, risk kültürü ve sürece yönelik gerekli tüm bilgilerin raporlanması

Bu bileşende, bilgi-işlem teknolojilerinin işletmenin her bölümünde güçlendirilmesi, kurumsal risk yönetimine yönelik iletişimin sağlanması, risk kültürü ve risk fakındalığının işletme içinde daimi olmasının sağlanması yer almaktadır. (Keskin 2016: 40.)

3.2.1.2.ISO 31000 Standardı

ISO, bağımsız ve sivil toplum örgütüdür. ISO, üyeleri vasıtasıyla gönüllülüğü artırmak, mutabakat tabanında yenilikleri destekleyen uluslararası standartlar hakkında ilgililere bilgi paylaşımı yapmak ve global sıkıntılara çözüm getirebilmek için alanında uzman birçok kişiyi bir araya getirmektedir. ISO'nun risk yönetimiyle ilgili teknik komitesi olan ISO/TC 262 tarafından risk yönetimine yönelik tüm faaliyetlerde uygulanması amacıyla bu standart geliştirilmiştir. Teknik uzmanların yaptığı toplantılardaki görüşmeler sonucunda birçok ülkede farklı işletmeler tarafından kullanılabilecek şekilde tasarlanmış ve sonrasında da revize edilmiştir. İlgili standart, çok sayıda ilke, detaylı bir risk yönetimi çerçevesi içermektedir. (Uysal 2018:58)

ISO 31000, işletmelerin risklerini etkili şekilde tanımlamalarını, kontrol etmelerini sağlayacak doğru risk yönetimi stratejisinin geliştirilmesine yardımcı olur. Böylece, işletmenin hedeflerine ulaşma ihtimalini artırmış ve varlıklarını koruyabilmesi için yön göstermiş olmaktadır. ISO 31000 içinde sadece riskler değil fırsatlarda değerlendirilmektedir. Normalde tüm ISO standartları beş yılda bir gözden geçirilmekte ve ardından gerekirse revize edilmektedir. ISO 31000 ilk olarak 2009 yılında yürürlüğe girmiş, 2018'de revize edilmiştir. İş dünyasında yaşanan gelişmelere uyum sağlamak ve yine yaşanan zorlukları bertaraf etmeye destek olabilmek amacıyla bu revize gerçekleşmiştir. Ekonomik sistemlerin öngörülemez oranda büyümesi, risk çeşitliliğinin günden güne artması revize ihtiyacının sebeplerinden biridir. ISO 31000'in 2018 revizesi, 2009'da ilk yayınlanan versiyonuna göre daha fazla stratejik yönlendirme içerir ve üst yönetimin risk yönetimi konusuyla daha fazla ilgilenmesini, bu şekilde de organizasyonda mevcut olan risklerin birbirleriyle bütünleşik şekilde ele alınmasını destekler. (Tranchard, 2018:. 2).

Standart, işletme bünyesinde kurumsal risk yönetimine doğru kaynak tahsisi yapılmasını, yetkili organlara gerekli sorumluluğun verilmesini öngören bir dizi düzenlemeyi içerir. Revize edilen standart; kurumsal risk

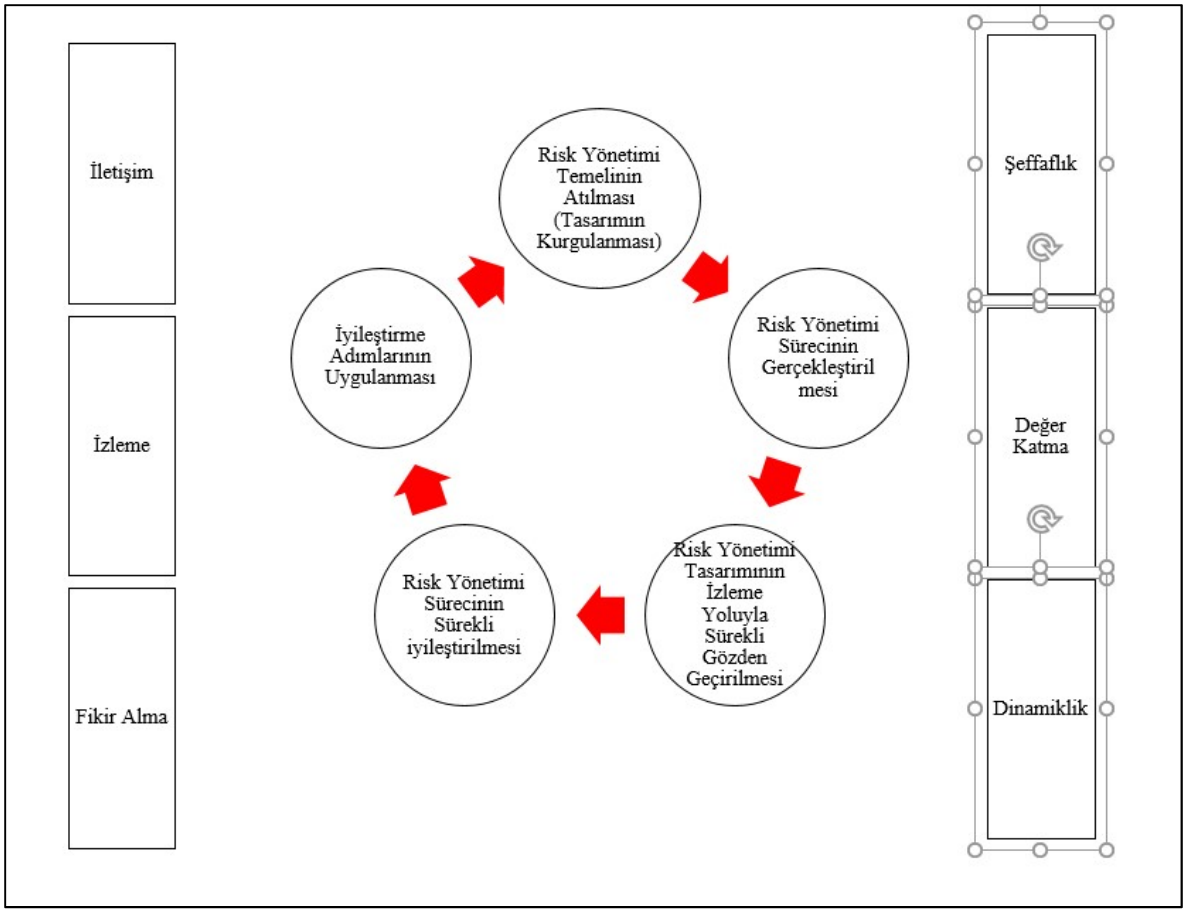
yönetiminin işletmelerde kurulması, yapısının oturtulması, işletmenin hedeflerinin/stratejilerinin ortaya konması gibi süreçlerinin yönetimine yönelik tavsiyeler içermektedir. ISO 31000'de de kurumsal risk yönetiminin ana noktası değer yaratma, sürekli iyileştirme, tüm paydaşların sürece dahil edilmesi şeklinde de ifade edilebilir.

Bu standart, işletmelerde sürekli gelişime, paydaşların sürece dahil edilmesine, insan ile ilgili ve kültüre yönelik faktörlerin dikkate alınmasına işaret eder ve risk yönetimi sürecinde değer yaratma üzerine odaklanır.

Bu bağlamda ISO 31000'de asıl amaç risk yönetimine yönelik aktarılmak istenen her noktanın çok basit ve anlaşılabilir şekilde ilgilenenlere/okuyanlara aktarılabilmesidir. Bu nedenle, kullanılan terminolojide oldukça kolay anlaşılır ve yanlış anlamaya mahal vermeyecek şekilde düzenlenmiştir. (ISO 2018)

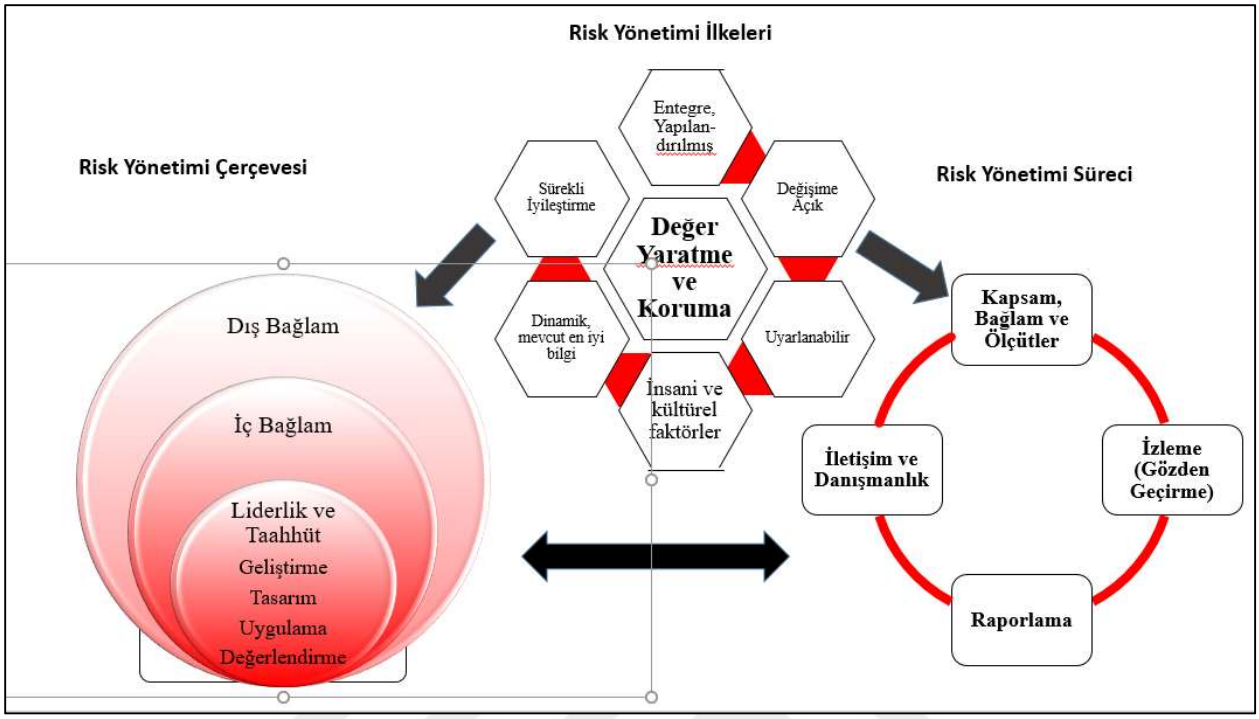
Standardın 2018'de yayınlanan yeni versiyonu, işletmelerde değer yaratan ve koruyanların kararlar vermek, hedefler belirlemek, bu hedeflere ulaşmak ve nihayetinde işletmenin performansını artırmak suretiyle riskleri yönetmeleri için bir çerçeve sunmayı hedeflemiştir.

ISO 31000 standardının ilk versiyonu (2009) ile güncellenmiş hali arasındaki (2018) ilişki ve farklılıklar aşağıdaki şekillerde gösterilmiştir.



Şekil 6. ISO 31000 Risk Yönetimi Çerçevesi (2009)

Kaynak: Yazar tarafından oluşturulmuştur.



Şekil 7. ISO 31000 Risk Yönetimi Çerçevesi (2018)

Kaynak: ISO 2018.

Yukarıdaki şekillere ve standardın içindeki ifadelere baktığımız da aşağıdaki çıkarımlar yapılabilmektedir:

2009'da yayınlanan standartta ilkeler; değer oluşturmaya yönelik, karar alma sisteminin bir parçası, sistematik, var olan bilgiye dayanan, insani ve kültürel faktörleri dikkate alan, dinamik, şeffaf ve kapsayıcıdır. 2018'de yayınlanan standart ise, bunlara ek olarak daha geniş, entegre, işletmelere göre özelleştirilebilen ve sürekli iyileştirme düsturunu da içermektedir.

2009 standardında oluşturulan çerçevenin sürekli takibi, iyileştirilmesi, yetkilendirme ve risk yönetiminin uygulanması varken 2018'de bu alan liderlik, adanmışlık, entegrasyon gibi kavramlarla tamamlanmıştır. Buradaki entegrasyon risk yönetiminin işletmenin tüm faaliyetlerinin içine entegre edilmesini anlatmaktadır. Ancak tam entegrasyon ve üst yönetiminde bu konuyu sahiplenmesi ile başarının geleceği vurgulanmıştır. (Uysal 2018:60-61)

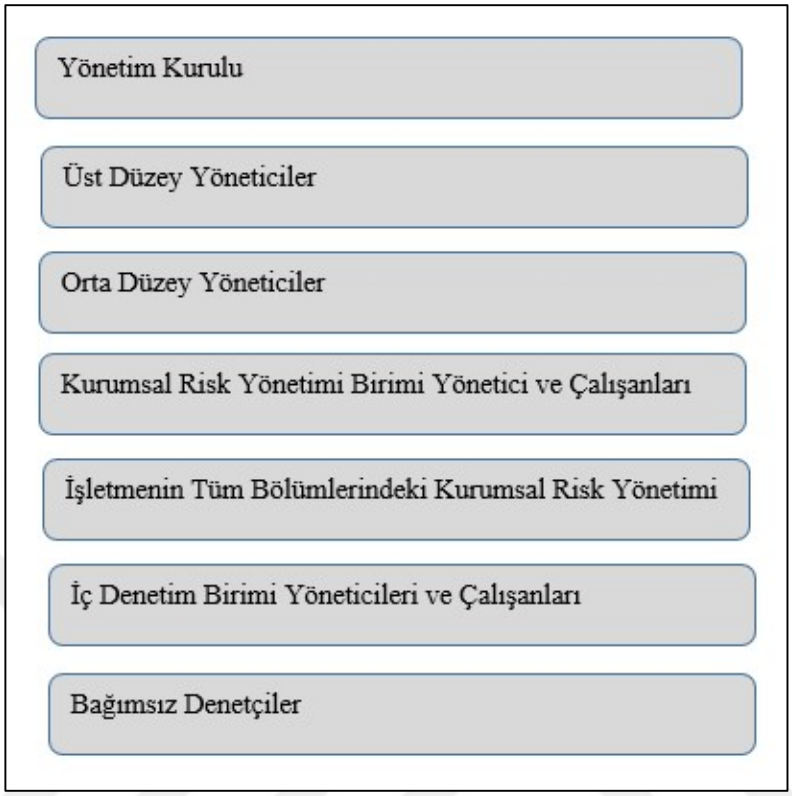
Süreç olarak karşılaştırdığımızda ise, ilk versiyonda risk yönetim sisteminin adımları daha sade halde yer alırken yeni versiyonda COSO'ya benzer bir adım silsilesi (Kapsamın belirlenmesi, risk değerlendirmesi,

izleme, gözden geçirme, iletişim, raporlama) olduğu görülmektedir. İçerik anlamında büyük bir fark göze çarpmamaktadır.

ISO 31000'in güncellenmesi de COSO güncellemesinde olduğu gibi, risk yönetiminin işletmenin tüm operasyonlarının içine entegre edilmesi ve üst yönetimin kurumsal risk yönetimini sahiplenmesi, sorumluluk alması esasına dayanmaktadır.

3.2.2. Kurumsal Risk Yönetiminde Roller ve Sorumluluklar

Risklerin yönetilmesinin sorumluluğu yönetim kuruluna aittir. Uygulamada, yönetim kurulu, risk yönetim çerçevesinin yönetimi ve işletimini çerçevede belirlenen görev ve etkililikleri gerçekleştirmekten sorumlu olacak bir yönetim ekibine devretmektedir. Bu faaliyetleri koordine eden ve yöneten, gerekli uzmanlık becerileri ile bilgi birikimini sağlayan ayrı bir bölüm veya fonksiyon da bulunabilir. Başarılı bir kurumsal risk yönetiminde normalde kurum içindeki herkesin bir rolü ve görevi vardır, fakat riskleri tanımlama ve yönetme sorumluluğu özel olarak kurum yönetimine aittir. Özet olarak, işletmenin her çalışanı kurumsal risk yönetimi konusunda sorumludur. Kurumsal risk yönetimi, CEO'nun sorumluluğundadır. Diğer yöneticiler, şirketin risk iştahı ile uyumlu olduğundan emin olmalı, sorumluluk alanlarındaki riskleri risk toleransları kapsamında yönetmelidirler. Genel olarak kurumsal risk yönetimi sürecinde risk yönetimi sorumlusu, mali işlerden sorumlu çalışan, iç denetçi ve diğerleri önemli görevler üstlenmektedir. İşletmenin diğer çalışanları, kurumsal risk yönetimi ile ilgili direktif ve protokollere uymak zorundadır. Kurumsal risk yönetimi, yönetim kurulu tarafından önemli ölçüde izlenmelidir. (Hazine Maliye Bakanlığı 2019:6-7)

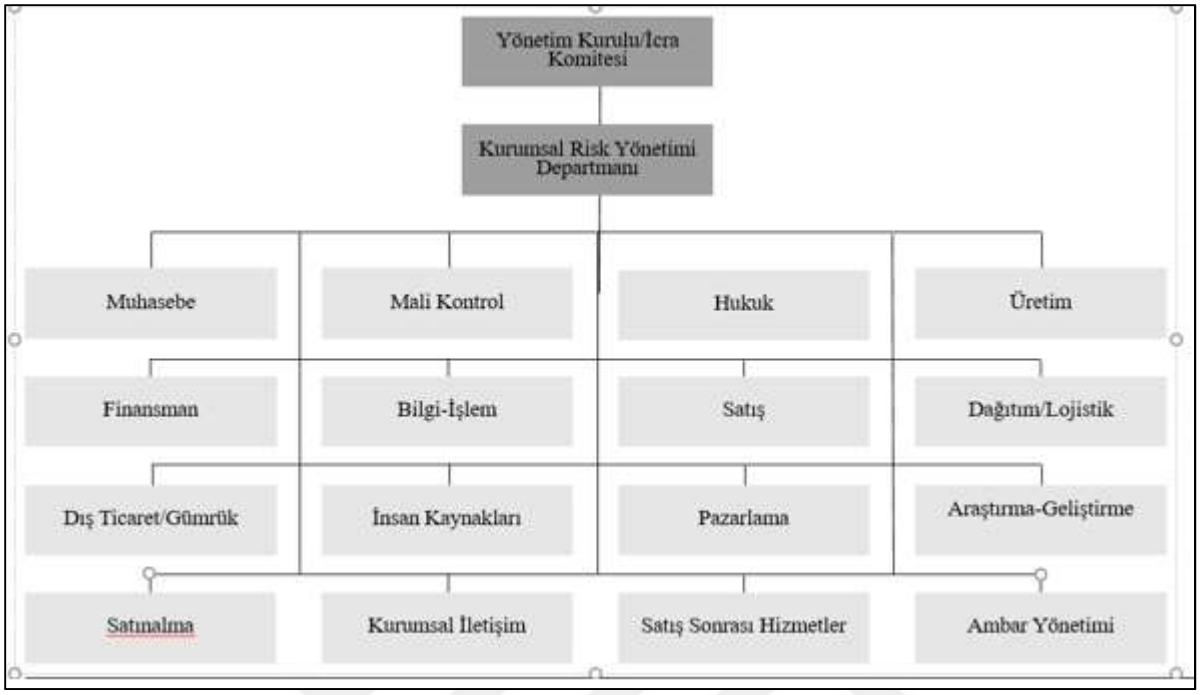


Şekil 8. Kurumsal Risk Yönetiminde Yetkili Kişiler

Kaynak: Yazar tarafından oluşturulmuştur.

Yukarıdaki şekilde bağımsız denetçiler dışındaki herkes işletmenin bünyesinde görev almaktadır. Ayrıca şekilde yer verilmemiş olsa da bir işletmeye kurumsal risk yönetiminin fayda sağlayabilmesinin en önemli koşulu işletmenin her kademesinde çalışan her personelde risk farkındalığının yaratılmış olmasıdır.

İşletmelerde tercihen kurumsal risk yönetimi sürecini yürüten ekibin yönetim kuruluna raporlaması sürecin işleyişi açısından uygun görülmektedir. Örneğin aşağıdaki şekilde görülen organizasyon şemasına sahip olan işletmelerde kurumsal risk yönetiminden sorumlu tek bir bölümün olmasının da etkisiyle KRY işlevleri kolaylıkla yerine getirilebilmektedir. Süreç içinde hem üst yönetim ile hem de operasyonda yer alan tüm bölümlerle açık ve sürekli iletişim halinde olması, bölümlerde çalışan her personelden gelebilecek olan risk bildirimlerinin değerlendirilip kurumsal risk yönetimi sürecine dahil edilmesi, belli periyotlarda üst yönetime gerekli raporlamaların yapılması da prosesin sağlıklı yürümesine katkı sağlayacaktır.



Şekil 9. Kurumsal Risk Yönetimine Yönelik Örnek Organizasyon Modeli

Kaynak: Yazar tarafından oluşturulmuştur.

Etkili kurumsal risk yönetiminin en önemli bileşenlerinden biri de roller ve sorumluluklar konusudur. Kişilerin rollerinin ve sorumluluklarının net bir şekilde belirlenmiş olması ve ilgililere ifade edilmiş olması gerekir. Konu tabii ki roller ve sorumluluklar dağıtıldığında bitmez, herkesin kendi rolünü gerçekleştirip gerçekleştirmediği, sorumluluklarını layıkıyla yerine getirip getirmediği risk yönetimi departmanı tarafından takip edilmelidir. İşletmelerdeki her çalışan ise, oluşturulan prosedürlere uygun olarak risk yönetimi sürecinin adımlarını eksiksiz uygulamakla yükümlüdür.

Bütün yöneticiler kendi bölümlerinde kurumsal risk yönetimi adımlarının doğru uygulanıp uygulanmadığını takip etmekle ve varsa eksiklikleri gidermekle sorumludurlar. Üst yönetim kademesi ise sistemin tamamının kurulması ve yönetilmesi ile sorumludur. Kendilerine bildirilen riskleri doğru değerlendirmeli, işletmenin geleceğini tehdit eden tüm olaylara titizlikle yaklaşmalı ve gerekli tedbirleri almalıdırlar.

Burada tabii ki değinilmesi gereken bir diğer konu iç denetim işlevidir. İç denetim birimi de risk yönetimi bölümünün süreci nasıl işlettiğini denetlemeli ve bu denetimin sonuçlarını üst yönetime sunmalıdır. Bu noktada denetim çıktıları büyük önem arz etmektedir.

21.yüzyılın gerekleri düşünüldüğünde tüm yöneticiler kurumsal risk yönetimini çok iyi bilmek ve uygulamak durumundadır. Organizasyonun her aşamasında yer alan çalışanların bu noktada üstlenmesi gereken sorumluluklar aşağıda yer almaktadır:

Yönetim kurulunun sorumlulukları: Yönetim kurulunun sorumlulukları, işletmenin büyüklüğü, gereklilikleri, kapsamı ile doğru orantılıdır. Yönetim kurulu, işletmenin kurumsal risk yönetimindeki gidişatını kontrol etmekten, gözetmekten sorumludur. Yönetim kurulunun bu noktadaki en önemli görevi, etkili bir kurumsal risk yönetimini işletmede tesis etmek ve uygulanmasını sağlamaktır. Bunu gerçekleştirebilmesi için sürecin en sonundaki risk raporlamasının da düzgün yapılıyor olması gerekir. Burada yönetim kurulu üyelerinin nesnel bakış açısına sahip ve sorgulayıcı olması çok kıymetlidir. (Özer, Erdem 2022:69)

Yönetim kurulunun şirketin stratejlerini belirleme, kurumsal risk yönetimi içeriğini oluşturma sorumluluğu vardır. Yönetim kurulunun risk yönetimi sorumlulukları; riskin stratejilerle olan bağını kurma, isk iştahı seviyelerini belirlemek, kurumsal risk yönetimi yapısını tesis etme, riskleri anlama, işletmeleri kriz anında yönetme olarak yer almaktadır. Yönetim kurulu belirli operasyonel riskleri değerlendirir, riskler içinde önceliği ve önemi yüksek olanları düzenli olarak takip eder, kabul edilemez risk statüsünde olan riskleri yani hem etkisi hem de gerçekleşme olasılığı yüksek olan risklerin etkilerinin en aza indirilmesine çalışır ve etkili bir kurumsal risk yönetimi sürecinin işletme içinde uygulanmasını güvence altına alır. (Deloitte, Global Risk Management Survey, 2019:16)

Üst düzey yöneticilerin sorumlulukları: Üst düzey yöneticiler, işletmenin özelliklerine göre, yönetim kurulunda yer alan genel müdür, genel müdür yardımcısı, direktör gibi unvanlar ile çalışan kişilerdir. Üst düzey yönetici, işletmenin kurumsal risk yönetimi konusundaki yeterliliklerini değerlendirmek zorundadır. Bu değerlendirme aşamasında ilgili tüm yöneticiler ve çalışanlarla görüşerek bu konudaki doğru bilgilere kısa zamanda erişir ve ona göre aksiyon alır. İşletmelerde bölümlerin yöneticileri risk ve fırsat içeren olayların belirlenebilmesi, risk değerlemesi yapılabilmesi için çeşitli teknikler geliştirirler. İşletmelerin ve daha özelde her bölümün kendi hedeflerine yönelik risk yönetimi prosedürlerinin geliştirilip

uygulanmasında, işletmenin operasyonlarının yürütülmesinden bilfiil ilgili yöneticiler sorumludurlar. Üst düzey yöneticiler, işletmelerin bel kemiğidir ve diğer yöneticilere liderlik ederler, işletmenin operasyonlarının yürütülmesinde karşılaşılabilecek olan tüm risklerin/fırsatların sürece dahil edilmesi konusunda koçluk yaparlar. Dolayısıyla sürecin sağlıklı uygulanmasında katkıları ve yönlendirmeleri çok kıymetlidir.

Yöneticilerin sorumlulukları: İşletmelerde her bölümün yöneticisinin kurumsal risk yönetimi sürecinde üzerine aldığı görevler vardır. Bunların en önemlisi, kendi bölümünde yürüyen her operasyonu kurumsal risk yönetimi açısından sürekli değerlendirmeye tabi tutması gerekliliğidir. Oluşabilecek her çeşit risk ve fırsata karşı uyanık olmalı ve bütün ekibinde de risk farkındalığını yerleştirmek için çalışmalıdır. (Özbek, 2012:276-280)

Kurumsal risk yöneticisinin ve kurumsal risk yönetimi çalışanlarının sorumlulukları: Kurumsal risk yönetimi politikasını işletmede tesis etme, işletmenin her kademesinde risk farkındalığının oluşturulması için çalışmalar yapma (düzenli eğitimler hazırlama/verme gibi), kurumsal risk yönetimi süreç adımlarını oluşturma ve sürekli gözden geçirme/güncelleme, sürece yönelik yönetim kuruluna önerilerde bulunma, sürecin son adımı olan risk raporlaması dahilinde gerekli dokümanları hazırlama meslek mensuplarının sorumluluk alanı içindedir.

İç/dış denetçilerin sorumlulukları: İç denetçiler, kurumsal risk yönetiminin etkililiğinin değerlendirilmesinde, sürece yönelik çeşitli önerilerde bulunulmasında önemli rol oynarlar. İç denetçiler, sürecin her aşamasında işletmelere/üst yönetime hem danışmanlık hizmeti verirler hem de güvence hizmeti sağlarlar. Sürecin kontrol ve izlemesini de yaparlar. İç denetçiler, risk değerleme ve risklerin sıralama faaliyetini güvence verme fonksiyonu çerçevesinde incelerler. İç denetçiler, kurumsal risk yönetiminin her aşamasında yapılması gerekenlerin doğru, etkili ve zamanında gerçekleştirilip gerçekleştirilmediğini tespit etmek üzere çalışmalarını yürütürler. Bu çalışmaların neticesinde de yönetim kuruluna hazırladıkları denetim raporlarını sunarlar. Bu rapor aracılığıyla eksik/hatalı olan konular hakkında geri bildirim verirken aynı zamanda da sürece ve sisteme yönelik önerilerde bulunurlar. (Özbek, 2012:276-280)

Özetlemek gerekirse, kurumsal risk yönetiminde her çalışan kendi görevlerinin yanında aynı zamanda çalıştığı her alanda risk sorumlusu olarakta kendini hissetmelidir. İşletmelerde tüm birimler/çalışanlar işlerine risk farkındalığı ile yaklaşmalı, risk raporlarını takip etmeli, kendi bölümlerinde olmayan ancak

başka bölümlerde ortaya çıkan risklere bakarak gerekli tüm önlemleri almalıdırlar. Bu noktada bölümler arası iletişim, yönetimin kurumsal risk yönetimine karşı doğru proaktif yaklaşımı geliştirmiş olması ciddi önem arz eder. (Sarıtaş, Kaya, 2017: 220).

3.2.3. Kurumsal Risk Yönetiminde Olgunluk Düzeyleri

Uluslararası İç Denetçiler Enstitüsü'nün kapsamlı tanımına göre risk olgunluğu; "İşletmenin hedeflerine etki eden fırsat ve tehditlere yönelik karşı tutumları tanımlamak, değerlendirmek, kararlaştırmak ve raporlamak üzere işletmenin her kademesinde ve noktasında sağlıklı ve sağlam bir risk yönetimi yaklaşımının yönetim tarafından benimsenme ve planlandığı gibi uygulanma kabiliyeti ve derecesidir."

Risk olgunluğu, bir işletmenin riski ne kadar iyi tanımladığı, değerlendirdiği, yönettiği ve izlediğinin bir ölçüsüdür. Sözkonusu işletmenin risk yönetimi uygulamalarının kalite ve entegrasyon düzeyini ifade eder. Yüksek düzeyde risk olgunluğuna sahip bir işletme, risk bilgisine dayalı kararlar almada ve istenen sonuçlara ulaşmada çok daha etkili olacaktır.

İşletmenin risk olgunluk düzeyinin belirlenmesinin işletmeye getireceği birçok fayda mevcuttur. Bunlardan bazıları aşağıda sıralanmıştır:

- Riske dayalı karar alma ve strateji belirlemeyi mümkün kılmak.
- İşletme genelinde iletişim ve istişarenin arttırılması.
- Ortak bir risk dili aracılığıyla riskler, fırsatlar ve stratejiler arasında bağlantı ve içgörü oluşturmak.
- Üst düzey yönetimin ve yönetim kurulunun yönetimin yönlendirmeleri konusunda iyi bilgilendirilmesi için risk yönetimi faaliyetlerinin dokümantasyonuna ve zamanında raporlanmasına olanak sağlamak.
- İşletmenin stratejik hedeflerine ulaşma olasılığını arttırmak.
- Paydaşlar için değer yaratmak ve bu değeri korumak. (IPPF, 2019:5)

Düşük seviyeye sahip işletmelerde, iç denetçilerin danışmanlık hizmeti vermeleri ve işletmenin risk yönetimi olgunluk düzeyini yükseltmeleri beklenmektedir. Zaten risk odaklı iç denetimin gerçekleşebilmesi için işletmenin mutlaka yüksek seviyede risk olgunluğuna erişmiş olması gerekir.

Kurumsal risk yönetimi süreci denetiminde iç denetçiler danışmanlık faaliyeti kapsamında iyileştirmeler önererek risk olgunluğunu yükseltmeyi hedeflerler. Ancak bu süreçte aşağıdaki örneklerde olduğu gibi, bazı zorluklarla karşılaşabilirler:

- Risk değerlendirmeleri çok fazla zaman alır.
- Kendilerine verilen risklere yönelik bilgiler geçerli/doğru veriler değildir.
- Risklere yönelik bilgiler/değerlendirmeler, işletmenin karar alma mekanizmasında kullanılmamaktadır. (IPPF, 2019:5)

İç denetim faaliyeti, kurumun risk yönetimi sürecine ilişkin bir değerlendirme tasarladığında, kurumun risk yönetimi olgunluk düzeyini ve risk kültürünü anlamak, uygun sorgulamanın geliştirilmesi açısından oldukça kıymetlidir. Eğer işletme, risk yönetimi bakış açısını veya felsefesini henüz tam olarak geliştirmemişse; iç denetim faaliyeti, bulguları ve tavsiyeleri formüle etmeden önce bunun nedenlerini anlamalıdır. Risk yönetimi sürecinin doğru bilgiyi verip vermediğine ilişkin görüşler önemlidir. Üst yönetim; risk yönetimi sürecinin onu yürütmek için gereken kaynaklara değmeyen bürokratik bir uygulama olduğuna inanırsa, o zaman büyük ölçekli iyileştirmeler önermek için erken olabilir. Çünkü büyük ihtimalle işletme bu önerilere şüpheyle yaklaşabilir ya da tamamen reddedebilir. Bunun yerine iç denetçiler kurumun risk kültürüne yönelik tavsiyelerde bulunarak işe başlamalıdırlar.

Bir işletmenin risk yönetimi olgunluk modeli konusundaki konumunu belirlemek ve risk yönetimi sürecinin kuruma ne kadar etkili bir şekilde hizmet ettiğini değerlendirmek için iç denetçiler çeşitli unsurları dikkate almalıdır.

Tüm işletmeler, farkında olmasalar ve doğru dokümantasyonu yapmıyor olsalar bile bir tür risk yönetimi süreci içindedirler. Belgelendirilmiş risk yönetiminin en basit biçimi, en üst düzeyde bir kurumsal risk kaydı oluşturmaya yönelik yıllık bir uygulamadır. Buna, üst yönetimin bir risk listesi geliştirip belgelediği ve değerlendirmenin bir sonraki yıla kadar tekrar ele alınmadığı "stratejik risk değerlendirmesi" adı verilebilir. Yelpazenin diğer ucunda, en sağlam veya olgun risk yönetimi sürecine sahip işletmeler, işletme genelinde kültürel veya yönetişim niteliğindekiler de dahil olmak üzere tüm risk faktörlerini sistematik, yapılandırılmış bir formatta değerlendirirler. (IPPF, 2019:6)

Aşağıdaki şekilde risk yönetimi sürecinin olgunluk düzeylerini ve her düzeyin detaylı açıklamalarını görülmektedir:

Tablo 7: Risk Yönetimi Olgunluk Düzeyleri

Düzey I- Riskten Habersiz	Risk yönetimi sürecinin gelişiminin erken aşamalarında olduğu organizasyonlarda, iç denetim faaliyeti, sürecin daha olgun olduğu zamana göre daha aktif bir şekilde faaliyet göstermelidir. Bu olgunluk düzeyinde, belirli risk yönetimi faaliyetleri; iç kontrol, uyumluluk, hukuk gibi fonksiyonlardan sorumlu operasyonel yönetim tarafından yeterli şekilde yerine getirilmiyor olabilir. Bu nedenle, bu tarz işletmelerde ilgili fonksiyonlar, iç denetim faaliyetinin risk değerlendirmelerine ve riske dayalı güvence ve tavsiyelerine ciddi ihtiyaç duyacaktır.
Düzey II- Riskin Farkında	Bu seviyede, iç denetim faaliyeti daha iyi organize olabilir, yeterli kaynak sağlanabilir ve daha kapsamlı risk değerlendirmesi yaparak süreçte önemli bir rol oynar. İç denetim faaliyeti; kontrol, uyumluluk, hukuk ve kalite güvence fonksiyonlarıyla birlikte çalışabilir ve yönetim fonksiyonlarındaki risk sahiplerinin operasyonel kontrolleri oluşturmasına ve izlemesine yardımcı olmak için iç denetim uzmanlığını kullanarak onlara katkıda bulunur. Süreç tutarlı, verimli bir şekilde çalışıyorsa ve işletmenin hedeflerine ulaşmasına yardımcı olacak eyleme geçirilebilir sonuçlar sağlıyorsa, bu aşama birçok işletme için yeterlidir.
Düzey III- Risk Tanımlanmış	Risk olgunluk modelinin ortasında yer alan işletmeler, tüm olgunluk düzeylerinin bir karışımı olarak görülebilir. Bu işletmelerde, genellikle bazı bölümler diğerlerinden daha yüksek olgunluk düzeylerinde faaliyet göstermektedir. Bu tür yapılarda, işletmenin kontrol, uyumluluk, hukuk ve kalite güvence fonksiyonları, belirli bir risk yönetimi sürecine sahip olabilir ve bunların bazıları da çok iyi yönetilen, optimize edilmiş seviyelere bulunabilir. Kontrol ve güvence fonksiyonları, operasyon yönetiminin riskleri değerlendirmesi ve diğer risk yönetimi faaliyetlerini gerçekleştirmesine

	yardımcı olmada aktif bir rol oynayabilir. İç denetim faaliyeti bu düzeyde işlevsel olarak rahatlıkla çalışabilmektedir.
Düzey IV- Risk Yönetiliyor	Yüksek risk olgunluk düzeyine ulaşmış işletmelerde; operasyonel yönetim, işletme genelindeki tüm riskleri sahiplenir, yönetir ve süreç içinde düzeltici eylemlerin gerçekleştirilmesinden de sorumludur. Bu tip işletmelerde; iç denetim faaliyeti, işletme yönetiminin kendi kontrollerinin ötesinde risk yönetimi sürecinin etkililiğini değerlendiren bağımsız bir güvence fonksiyonu olarak hareket eder.
Düzey V- Risk Optimize Ediliyor	En üst olgunluk düzeysine ulaşmış işletmelerde, operasyonel yönetim, risk yönetimi sürecinin sahibidir. İşletmenin uyumluluk ve/veya risk yönetimi fonksiyonları, işletmenin kendi menfaati için risk değerlendirmelerini gerçekleştirir. Ayrıca operasyonel yönetim tarafından üretilen risk değerlendirmeleri izlenir, raporlanır ve ihtiyaç halinde risklere yönelik müzakereler yapılabilir. İç denetim, bu olgunluk düzeyinde rahatlıkla işletmenin kendi risk yönetimi sürecine yönelik tüm raporlarını etkili şekilde kullanabilir.

Kaynak: IPPF 2019: 7-8

Risk yönetimi olgunluk düzeylerinin belirlenmesindeki en önemli ölçütler; risk iştahının ne şekilde belirlendiği ve bu bilginin işletme içinde ilgili kişilerle paylaşılıp paylaşılmadığı, risk değerlendirmesi aşamasının hangi şartlar altında, hangi belgeler ve hesaplama yöntemleri ile yapıldığı, işletmede risk yönetimine yönelik ortak bir dilin olup olmaması, risk yönetimine yönelik bilgilendirme ve iletişimin nasıl yapıldığıdır Bu noktada, işletmedeki risk kültürü ve risk farkındalığı büyük önem arz etmektedir. (IPPF, 2019:8-9)

İşletmelerin riski ölçmek ve değerlendirmek için detaylı süreçleri olabilir ama kültür bu süreci desteklemeyebilir. Operasyonel bir risk yönetimi sürecine sahip olmanın gerekli olduğu işletmelerde,

yönetimin odak noktası yalnızca bir kontrol listesindeki kutuları işaretlemekse, risk yönetimi sürecinin, risk bilgilerinin karar alma sürecine entegre edildiği bir olgunluk düzeyine ulaşması pek mümkün değildir.

Eğer iç denetçiler işletmede etkili olabilecek bir risk yönetimi sürecinin tasarlanmasına dahil olursa ve onların bu çabasına rağmen işletmenin kültürü bu adımları desteklemiyorsa, bu konuyu üst düzey yönetim ve yönetim kurulu ile sürecin uygulanabilirliğini tartışabilecek olan ortamlara getirmeleri gerekir. Üst yönetimin tavrı risk yönetimi sürecinin destekliyor gibi olsa da, organizasyonda bu kabulün gerçekleşmesinin tek yolu üst yönetimin risk yönetimin gerekliliğinin anlaması ve o farkındalık aşamasından sonra ilgili sürecin işletmede etkili şekilde uygulanması için gerekli tedbirleri almasıdır.

İç denetim, işletmelerin beklenen risk yönetimi olgunluk düzeyine çekilmesi için danışmanlık ve güvence hizmeti ile onlara destek olmaktadır. İç denetimin bu çabası, işletmenin kendi dinamiklerinin de aynı yönde ilerlemesi halinde sonuca ulaşacak ve her işletme kendi şartlarına, sektörüne, büyüklüğüne göre bir olgunluk düzeyine yerleşecektir. Burada her işletmenin en yüksek olgunluk düzeyinde olmasının gerekmediğinin de unutulmaması gerekir.

3.2.4. Kurumsal Risk Yönetimi Uygulamalarında Yaşanabilecek Riskler

Amerika'da yayınlanan Sarbanes Oxley Kanunu'nun etkisiyle kurumsal risk yönetiminin detaylı şekilde herşeyin risk yönetimi şeklinde algılanması ve bu doğrultuda uygulanmasının negatif sonuçları olabileceği yönünde iddialar bulunmaktadır.

Mevcut kurumsal risk yönetimi çerçevelerinin tarif ettiği şekilde, işletmeler her şeyin risk yönetimi anlayışı ile yönetildiğinde birçok sorunla karşı karşıya kalabilmektedirler. Bu yöntemde karşılaşılma ihtimali olan önemli, önemsiz, gerçekleşme olasılığı düşük-yüksek her risk sistem içinde değerlendirilmekte ve yöntem samanlıkta iğne aramaktan farksız hale gelmektedir. Bu gibi yan etkiler ortadan kaldırabilmek için 80/20 Kuralı (Pareto Prensibi) uygulanabilir. Bu kural uyarınca, sonuçların %80'inin kaynağı bu sonuçların nedenlerinin %20'sidir. Başka bir deyişle, elde edilecek faydanın büyük kısmı harcanan eforun göreceli olarak daha küçük bir yüzdesinden elde edilir. Kurumsal risk yönetimi açısından bu kuralı düşündüğümüzde, bir işletmenin hedeflerine ulaşmasını etkileyecek risklerin %80'ine, mevcut süreçlerin sadece %20'sine denk gelen ve gerçekten kritik olarak görülebilecek olaylar neden olmaktadır. Bu yüzden, etkili bir kurumsal risk yönetimi stratejisi geliştirebilmek ve riskleri/fırsatları etkili şekilde yönetebilmek için işletmeler her şeyin risk yönetimi anlayışı yerine işletmenin kendi yolculuğunda sürdürülebilirliğini

tehlike altına sokacak zorlukları belirlemelidir. Önemli/ önemsiz diye düşünmeden tüm süreçleri sürekli kurumsal risk yönetiminin her aşamasında incelemek risk yönetimi çalışmalarının etkililiğini azaltmakta ve çalışanlar/yöneticiler açısından bu çalışmaların sadece bir iş yükü olarak görülmesine sebep olmaktadır. (Kıral 2018:10).

Günümüzde risk yönetimi, işletmelerin karşı karşıya kaldıkları belirsiz durumları önceden daha tahmin edilebilir hale getirmek ve karşılarına çıkmayacak olan olası durumları da göz önüne alarak bir kurumsal yapı içinde uygulamak durumundadır. Bu noktada meydana gelen belirsizliğin derecesinin belirlenmesine yönelik metaforik bir kavram ortaya atılmıştır. Siyah kuğu (black swan) olarak isimlendirilen bu teoride işletme içerisinde kurumsal risk yönetimi ne kadar düzgün uygulanırsa uygulansın bazen tahmin etmesi güç olaylarla karşılaşıldığında işletme zor durumda kalabilmekte ve operasyonları aksayabilmektedir. (Locklear, 2012: 14). Buradan çıkarılabilecek sonuç, işletmelerin her durumda her türlü sıkıntıya ve zorluğa hazır olacak şekilde kendilerini geliştirmiş olmalarının gerekliliğidir.

Sadece kurumsal risk yönetiminin uygulanmasında değil iç denetiminde de bazı sıkıntılar yaşanabilmektedir. Bu sıkıntıların azaltılmasına yönelik olarak yapılması gereken ilk şey, iç denetçilerin kurumsal risk yönetimi çerçevesini iyi anlamaları gelmektedir. İç denetçiler, genellikle iç kontrol adımlarının yeterliliğine odaklanırlar. Başka bir deyişle, iç kontrol sisteminin yeterli olmasını riskleri minimize eden bir olgu olarak kabul ederler. Ancak COSO 2017'de merkezde yer alan kavram iç kontrol adımları değil "risk" kavramıdır. İç denetim birimleri, riski tanımlamalı, değerlendirmeli, analiz etmeli, risk cevaplarını oluşturmalı ve gözden geçirip raporlamalıdır. Yine iç denetçiler zamanlarının çoğunun iç kontrol adımlarının etkililiğinin tespitine değil risk azaltmaya harcarlarsa işletmelerin hedef koyma ve bu hedeflere ulaşma yolunda karşılaşabilecek sıkıntıları azaltmış olacaklardır. Bu anlayışa hakim iç denetçi sayısı ne kadar artarsa, işletme üst yönetimleri de iç denetimin işletmeye katma değer yaratma konusundaki önemini daha iyi anlarlar. İç denetim esnasındaki sıkıntıları azaltmanın son yolu da, iç denetçilerin sadece iç kontrol adımları ve riskleri değil aynı zamanda yöneticilerin risklere verdikleri tepkileri de değerlendirmelerinin gerekliliğidir. Bu şekilde, iç denetçiler yöneticilerin bir riski ele alırken doğru yöntemi seçip seçmediğini de gözlemleme fırsatı bulurlar. Tüm bunlara ek olarak eğer iç denetçiler görevleri esnasında sadece riskleri değil fırsatlar üzerinde de çalışırlarsa işletmede meydana gelen olumlu-olumsuz tüm olayların işletmenin performansına olan etkisini daha doğru şekilde analiz etme imkanına kavuşurlar. (Anderson 2017, 43).

Sonuç olarak, riskler etkili bir risk yönetimi süreci içinde değerlendirildiği ve etkili şekilde denetlendiği sürece iş yaşamının doğal akışında korkulmaması gereken olaylardır.

3.3. Kurumsal Risk Yönetimi Süreci Ve İşletmelerdeki Uygulaması

Kurumsal risk yönetimi süreci, mutlaka sistematik ve devamlı bir süreç olarak işletmelerde oluşturulmalıdır. Risk ve fırsat yönetimi işletmelere yerleştirilirken değer yönetimi ve işletmeye katma değer yaratma konusu sürecin tasarım aşamasından son noktasına kadar dikkat edilmesi ve atlanmaması gereken çok önemli konudur. İşletmede herkesin organizasyona katma değer oluşturma fikri ile düşünmesi, davranması gerekmektedir. Burada dikkat edilmesi gereken noktalardan biri de risk ve fırsat yönetimi sürecinin mutlaka planlama ve kontrol sistemlerinin içine entegre edilmesidir. Ancak bu şartlar altında yaratılan süreçte sürekli izleme ve kontrol yapabilmek mümkün olur. Süreç içindeki adımlar yaşanırken özellikle de risklerin belirlenmesi ve değerlendirilmesi aşamalarında mutlaka etkili şekilde kullanılması gereken bazı araçlar vardır. Bunlardan bazıları plan-fiili analizleri, çeşitli dönemler ve raporlama grupları arasındaki sapma analizleridir. Bu analizler vasıtasıyla yapılacak olan karşılaştırmalar ile süreç sağlıklı şekilde yönetilebilir hale gelmektedir. Özellikle risk değerlendirme sonrasındaki kontrol, izleme, raporlama alanlarında kriz planlarının yapılması, önlem planlarının yapılıp sürekli takip edilmesi, bilgi işlem destekli çeşitli sistemler aracılığıyla hem raporlama yapılıp hem de bu raporların gerekli olan süre boyunca saklanabilmesi önem arz etmektedir. (Goetze, Henselmann:62-63)

3.3.1. Kurumsal Risk Yönetimi Süreci Hazırlık Aşaması (Bileşenler, Vizyon, Misyon)

Kurumsal risk yönetimi sürecinin adımlarına geçmeden önce bazı hazırlıkların yapılması gerekmektedir. Bu hazırlıkları iç ve dış unsurların belirlenmesi, işletmenin vizyonu/misyonu ile ilgili bilgi sahibi olma şeklinde ifade edilmektedir.

Kurumsal risk yönetim sisteminin işletmelerde tesis edilebilmesi için, öncelikle işletmelerin faaliyet gösterdikleri sektör, içinde bulundukları pazardaki konumları, sahip oldukları etik değerler, insan kaynakları politikaları, organizasyon şemaları, üst yönetimin idare şekli gibi konular hakkında yeterli bilgiye sahip olunması gereklidir. İşletmenin kendini tüm detaylarıyla tanımasının yolu açılmalıdır. (Kızılboğa, 2013: 204). Ancak bu şekilde işletme, kendi güçlü ve zayıf yönlerinin farkına varıp, kuvvetli taraflarını koruyup daha da güçlendirme ve zayıf yönlerini ise geliştirme imkanı bulacaktır. Tüm bu bileşenler kurumsal risk yönetimi sisteminin tesis edilmesi için bir temel teşkil eder.

İç unsurlar konusunda bilgi sahibi olunduktan sonra sıra dış unsurlara gelmektedir. Bunlar arasında, işletmenin faaliyette bulunduğu çevreyi (ekonomik, sosyal, siyasal), pazar koşullarını, rekabet ortamını ve işletme ile ilişki halinde olan tüm dış paydaşlara yönelik konuları sayabiliriz. Tüm bu bileşenlere yönelik bilgi sahibi olunduğunda işletmenin çevresinde mevcut olan riskler/fırsatlarda işletme yöneticileri ve denetçiler tarafından değerlendirilebilir olacaktır. (Saka, 2008). Dış unsurlar içinde üniversitelerle, sivil toplum kuruluşlarıyla, devlet kurumlarıyla, medyayla olan ve işletme faaliyetlerini etkileyen tüm ilişkiler yer alabilir. (Derici, 2015: 35). İşletmeler tespit etseler bile bu dış unsurların olumsuz etkilerini çoğunlukla yok edemeyebilirler. Ancak eğer bir işletmede etkili bir kurumsal risk yönetim sistemi mevcut ise, işletme yönetimi dış unsurlar kaynaklı olayların etkilerini karar alma mekanizmalarında verimli şekilde kullanabilirler. (Usman, Kaygusuz, 2019: 115)

Kurumsal risk yönetiminin uygulanması sürecinde işletmede faaliyette bulunan tüm çalışanların işletmenin vizyonu ve misyonu hakkında bilgi sahibi olması, işletmenin hangi hedeflere doğru ilerlemek istediğini anlaması, benimsemesi çok önemlidir.

İşletmenin bel kemiği vizyonu ve misyonudur. Vizyon, işletmenin gelecekte nasıl bir konuma varmak istediğini bize ifade etmektedir. Her işletmenin kısa ve uzun vadeli hedefleri vardır. Uzun vadeli hedefler aslında bize vizyonu yansıtır. İşletmenin durumuna uygun şekilde belirlenen bir vizyon, işletmeye yol gösterir, işletmenin çalışanlarının gözünde onları motive edebilecek bir resim yaratır. Vizyon, bir çeşit yol haritasıdır. Misyon ise işletmenin var olmasının sebebidir, en temel amacıdır. Kurumsal risk yönetimi sürecine hazırlık aşamasında vizyon ve misyon elden geçirilmelidir. İşletmenin kurumsal kimliği ile bağdaşmayan noktalar tespit edilirse hemen düzeltilmelidir. (Kızılboğa, 2013: 204).

3.3.2. Kurumsal Risk Yönetimi Sürecinde Mevcut Durum Analizi ve Strateji, Hedef Oluşturma

Bunun yanı sıra mevcutta kullanılan kurumsal risk yönetim sisteminin durumunun incelenmesi de yeni sürece hazırlık aşamasında öncelikle yapılması gerekenler arasında yer almaktadır.

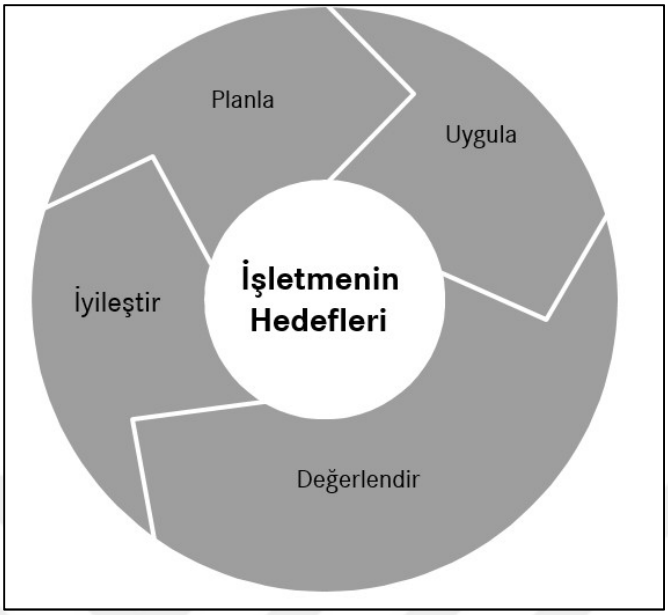
Mevcut durum analizinde öncelikle ayrıntılı bir inceleme yapılır, risklere yönelik oluşturulan sistem analiz edilir, işletmenin risk portföyü çıkarılır. Bir çeşit haritalama yöntemi ile bu analizin tamamlanması işletmeye fayda getirmektedir. İncelemeler bittikten sonra, mevcut sistemin olumlu ve olumsuz yönleri ortaya konmaktadır. Bu noktada risk yönetimine dair bilgilerin kimlerden toplandığı da önemli bir ölçüttür.

Tek bir birimden veri alınabiliyorsa entegre bir kurumsal risk yönetiminden pek söz edilemez. İşletmenin her departmanında bu bilgiler mevcut ise ve risk farkındalığı varsa o zaman eldeki mevcut durumun da oldukça iyi bir seviyede olduğu kabul edilebilmektedir.

Mevcut durum analizini takip eden adım ise işletmenin hedeflerinin net şekilde belirlenmesidir.

İşletmelerin kurumsal risk yönetimi sürecini tasarlayabilmek için öncelik risk profillerini tanımlaması ve dolayısıyla işletme stratejilerinin belirlenmesi gerekir. Zaten COSO 2017 ile de stratejilerin önemi ve işletmeye değer yaratmanın altı çizilmiştir. İşletme stratejileri, işletmenin mevcut durumu analiz edildikten sonra hedeflerine ulaşmasını sağlayacak şekilde oluşturulmalıdır. (TÜSİAD, 2008: 34). Stratejiler netleştirildikten sonra hedef belirleme aşamasına geçilebilmektedir. Hedef belirleme, işletmelerde üst yönetimin işletmenin misyonu, vizyonu, belirlenen risk iştahı ile orantılı şekilde işletmenin gideceği yolu belirleyeceği süreçtir. (Mattie ve Cassidy, 2008: 4). İşletmelerin hedefleri genelde dört grupta toplanır. Bunlar, stratejik hedefler, operasyonel hedefler, raporlama hedefleri ve uygunluk hedefleridir. (COSO, 2004:37). Stratejik hedefler yönetim kurulunun belirlediği üst düzey hedeflerdir. İşletmenin kaynaklarının verimli kullanılmasıyla tüm faaliyet alanlarını kapsayan hedefler, operasyonel hedefler olarak ifade edilebilir. İşletmenin yönetim kurulu ve üst düzey yöneticilerine zamanında ve doğru kararlar alabilmeleri için gerekli olan bilgilerin sağlanması raporlama hedefleri olarak geçer. İşletmenin içinde yer aldığı pazar ve pazar şartları, fiyatlandırma politikaları, vergilendirme, çevrenin korunması gibi konularla ilgili tüm düzenlemelere yönelik hedeflerde uygunluk hedefleridir. Bu şekilde işletmenin hedeflerinin gruplara ayrılması ve ayrı ayrı bu hedefler üzerinde çalışılması kurumsal risk yönetimine geniş bir bakış açısı getirebilmektedir. (Ekici 2015: 92-93). İşletme hedeflerinin net, herkes tarafından kolay anlaşılır, ölçülebilir, güncel ve gerçekçi şekilde tahsis edilmesine önem vermek gerekir. (Burnaby ve Hass, 2009: 545)

Bu noktada belirlenen tüm hedefler dönem dönem kontrol edilmeli ve güncellenmelidir ve gerçekçi, ulaşılabilir olduğundan emin olunmalıdır. İşletmede hedefler belirlendikten sonra mutlaka bu hedeflerin çalışanlarla iletişimi yapılmalı, onlara anlatılmalıdır. İşletmelerde her kademedeki çalışanın vizyon, misyon, strateji ve hedefler hakkında yeterli, gerekli bilgiye sahip olmaları işletmede etkili bir iç kontrol mekanizmasının kurulması, iyi çalışan kurumsal risk yönetimi sistemi tesis edilmesi açısından büyük önem arz etmektedir.



Şekil 10: İşletmelerde Hedef Belirleme Süreci

Kaynak: Yazar tarafından oluşturulmuştur.

Hedefler üzerinde yapılması gerekenler tamamlandıktan sonra işletmede tercih edilebilecek risk stratejileri üzerinde görüşmek, değerlendirmeler yapmak gerekir. Bunlar aynı zamanda kurumsal risk yönetiminde kullanılacak yöntemler/tekniklerdir. Risk yönetimi teknikleri arasında riskten kaçınmak, riski almak, riski azaltmak yer almaktadır. İşletmeler, içindeki bulundukları şartlara bakarak bu konuda kararlarını vermelidir. Bazı konulardaki riskler, işletmenin beraber çalıştığı sigorta firmasıyla beraber yönetilebilir ya da çok ortaklı işletmelerde ana şirketin veya grup içindeki başka bir şirketin bu riski taşıması daha doğru olmaktadır.

Sigortasız kayıpların tazmin edilmesi için bütçeden ayrılan bir fon kullanılabilmektedir. Bu aşamada risk yönetim sürecinin tam olarak her bir riskle mücadele etmek için hangi yöntemin kullanılacağını belirlemek oldukça zordur. Bu kararlar, işletmeler arasında değişkenlik gösterir. İşletmelerin yönetim politikası katı ve kapsamlı olduğunda, risk yönetimi karar verme aşamasında oldukça sınırlı kalabilir. Risk yöneticisi, programın yapıcısı olarak değil, programın uygulayıcısı olarak çalışabilir. Risk yöneticisi, hangi tekniğin daha uygun olduğunu belirlemek için potansiyel kaybı, ihtimalleri ve eğer kayıp olursa tazmin kaynaklarını hesaplamalıdır. Her yaklaşımın maliyeti ve kazancı ayrı ayrı hesaplanmalıdır.

Bu stratejilerin belirlenmesinde göz önüne alınması gereken en önemli ölçütler aşağıda yer almaktadır:

Riskin hasar derecesi: Karar alma mekanizmasında olanlar, beklenen kazançlara göre beklenen kayıpları da hesaplamalıdırlar. Bu nedenle risk değerlendirmesi yapılmalıdır.

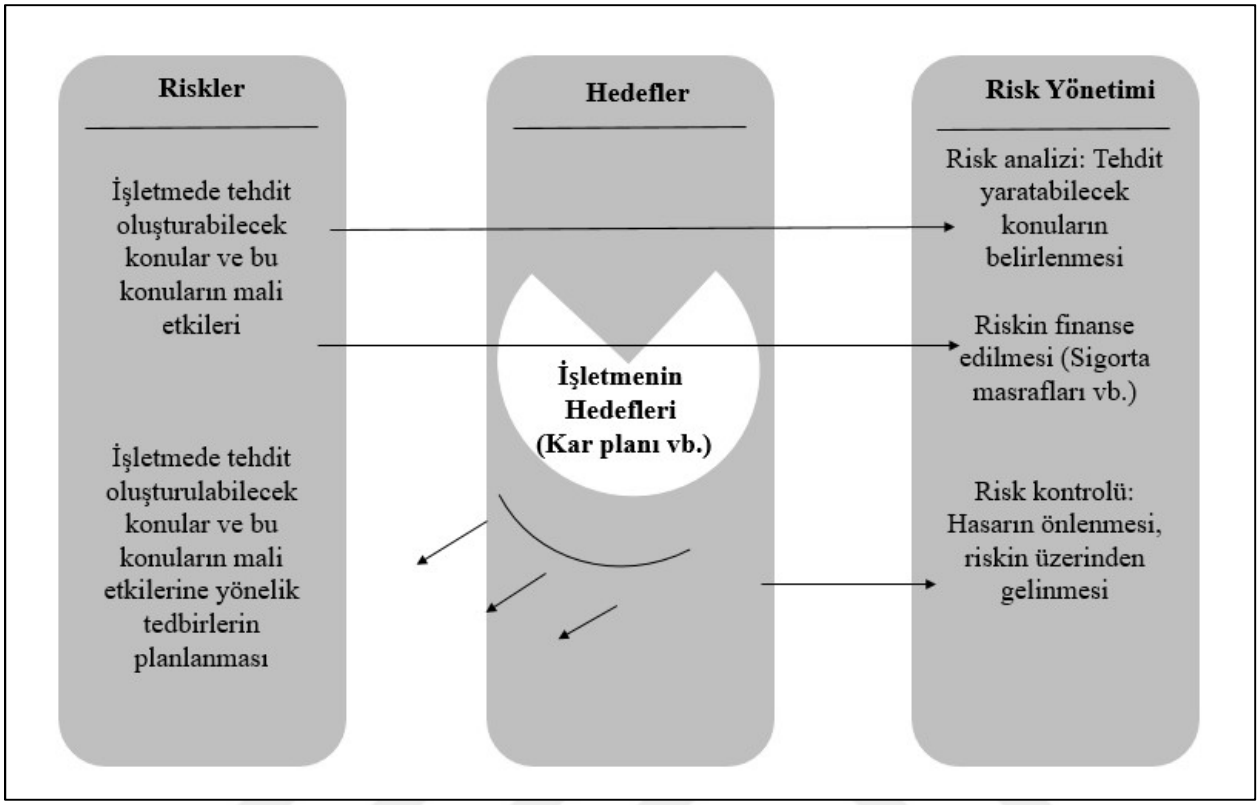
Ekonomik olması: Mümkün olan seçenekler arasından işletme için en iyisini belirlerken kullanılacak bütçe mutlaka dikkate alınmalıdır.

Zamanlama: Karar verilecek konunun aciliyetine ve önemine göre karar vermelidir. Acil konular hemen ele alınmalı, acil olmayanlar için ise daha uzun vadede karar alınabilir.

Kaynakların sınırlandırılması: İnsanlar organizasyonun en önemli kaynağı olduğu için en az işgücü gerektiren çözüm seçilmelidir. (Emhan 2006, 214-215).

Yukarıdaki ölçütlere göre değerlendirmeler yapıldıktan sonra, işletmenin operasyonlarını gerçekleştirmesi sırasında kaldırabileceği riskleri üzerine alması kabul edilirken, kaldırmaması gereken yani gereksiz riskleri üstüne alması da engellenmelidir. Burada hem riskin mali boyutu hem harcanacak işgücü dikkate alınmalıdır. Alınan riskler için mutlaka önlem planları tanımlanmalı ve bu önlem planları zaman içinde takip edilmelidir. Bu noktada fayda-maliyet analizi dikkatle yapılmalı, operasyona fayda sağlama ihtimali yüksek olan olaylarda oluşabilecek riskleri almaya dikkat edilmelidir. İşletmeye maddi-manevi fayda sağlamayacak alanlardaki riskleri almaktan kaçınılmalıdır.

İşletmenin hedeflerine ulaşabilmesi yolunda risk yönetiminin oynadığı kıymetli rolü aşağıdaki şekilde de görebiliriz:



Şekil 11: Risk Yönetimi Aracılığıyla İşletme Hedeflerinin Güven Altına Alınması

Kaynak: Hoffmann, K. 1985:8.

Karşı karşıya olunan risklerin işletmenin menfaatleri doğrultusunda makul seviyede tutulmasına ilişkin genel stratejiler belirlendikten sonra, bu stratejileri hayata geçirmek üzere gerekli olan politikaların belirlenmesi ve işletme içi kullanılacak yönergelerin hazırlanması gereklidir. Bu çalışmalar gerçekleştirilirken aşağıdaki noktalara dikkat edilmesinde yarar bulunmaktadır:

- Öz disiplin süreçlerinin tanımlanması, alt sistem olarak muhasebe, mali kontrol, raporlama, iç kontrol, iç denetim, kurumsal risk yönetimi ve kurumsal yönetim süreçlerinin entegre şekilde çalışmasının sağlanması
- Kurumsal risk yönetimi süreçlerinin etkili olarak uygulanmasını güvence altına almak üzere üst yönetim başta olmak üzere tüm personelin kurumsal risk yönetiminin önemine vakıf olması
- Kurumsal risk yönetiminin etkililiğin artırılmasına yönelik olarak muhasebe, raporlama ve kontrol süreçlerinde gerekli görülen tüm düzenlemelerin yapılması

- Kurumsal risk yönetiminin bağımsız şekilde gerçekleştirilmesini sağlayacak organizasyonel önlemlerin alınmış olması. (Coşkun 2009: 43-44)

3.3.3. Kurumsal Risk Yönetimi Sürecinde Performans Yönetimi

Kurumsal risk yönetiminde performans yönetimi denildiğinde, önem eşiklerinin belirlenmesinden başlayarak risklerin/fırsatların tespiti, verecekleri hasarın ya da getireceği pozitif olanağın belirlenmesi, gerçekleşme olasılıklarının ortaya konması, risklerin önceliklendirilmesi, risk cevaplarının ortaya çıkarılması anlaşılmaktadır.

3.3.3.1. Önem Eşiğinin Belirlenmesi

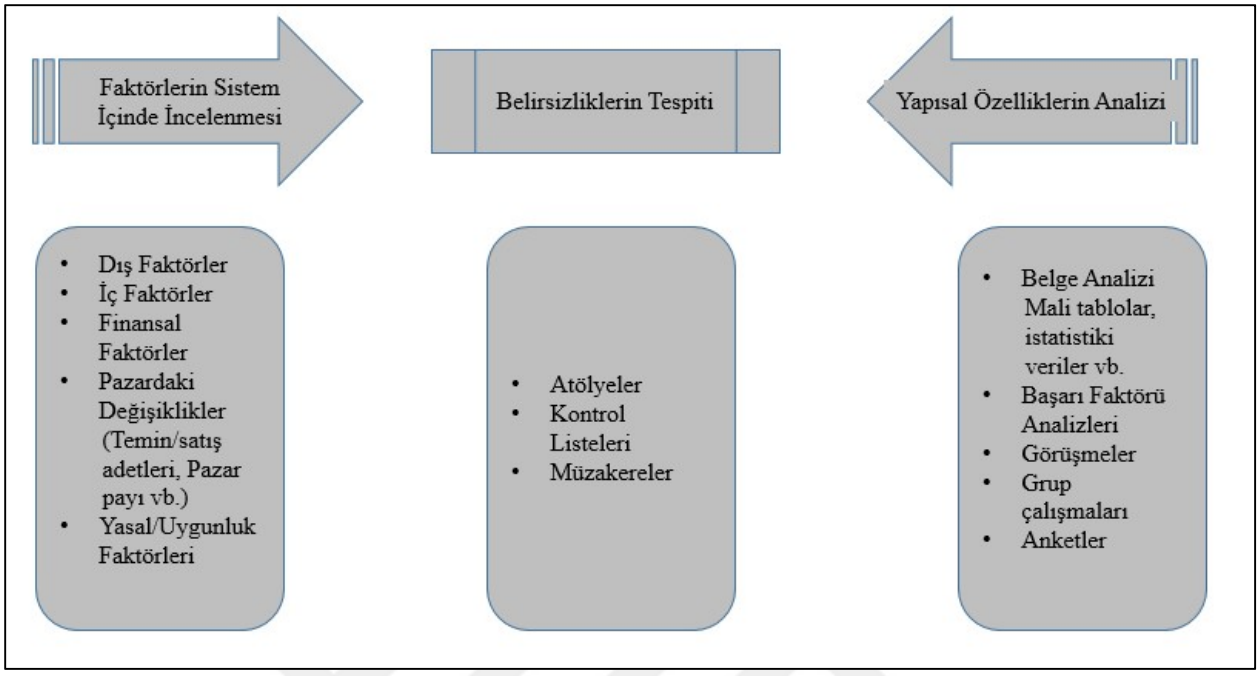
İşletmelerde önem eşiği olarak da ifade edilen ve risk iştahı ile de birebir bağlantılı olan bir kavram bulunmaktadır. Bu kavram bize söz konusu işletmenin hedeflerini gerçekleştirmesine engel olmayacak ve sürekliliğini tehlikeye sokmayacak tutardaki/orandaki risklerin belirlenmesi için kullanılır. Belirlenen tutar ne ise o tutarın altında olan riskler, işletme kendi faaliyetlerini yerine getirirken bir şekilde en aza indirgeyebileceği ve tehdit unsuru haline gelmeyecek risklerdir. Ancak önem eşiğinin üzerinde değerlendirilen riskler mutlaka çok yakın takibe alınmalı, bu risklerin doğuracağı olası zararların azaltılabilmesi için ivedilikle gerekli önlemler alınmalıdır.

3.3.3.2. Risklerin Belirlenmesi ve Vereceği Hasarın Tespiti

Kurumsal risk yönetiminin önem eşiklerinin belirlenmesi sonrasındaki ilk adımı risklerin tespit edilmesi ve detaylı olarak tanımlanmasıdır. Riskin tanımlanması sürecinde önemli olan belirsizliklerin ortadan kaldırılmasıdır. Çünkü belirsizliği yok etmeden risklere yönelik aksiyon almak mümkün olmayacaktır.

Eğer bir işletmenin risk profili oluşturulmak isteniyorsa, öncelikle risklerin tespiti ile başlamamız gerekir. Belirlenecek olan risklerin işletmenin hedefleri ile doğal olarak bağlantısı olması beklenmektedir. Bu riskler, risk çeşitlerinde anlatıldığı üzere iç riskler veya dış riskler olabilir. İşletmenin kendi iç dinamiklerinden kaynaklanan riskleri iç risk, işletmenin dışındaki olaylardan kaynaklı riskleri de dış risk olarak tanımlayabiliriz.

Risklerin ve şansların belirlenmesine yönelik olarak etkileşim şemasını aşağıda görebilirsiniz:



Şekil 12: Risk/Fırsat Belirleme EtkileşimTablosu

Kaynak: Goetze, U., Henselmann, K. 2001:23.

Yukarıdaki şekilde de gösterildiği üzere, dış faktörler içinde politik gelişmeler, teknolojik gelişmeler, yasal değişiklikler sayılabilirken iç faktörler olarakta işletmenin kendi üretim hacminde olabilecek değişiklikler, organizasyonel konular gibi meseleler yer almaktadır. Rekabet durumundaki değişiklikler, tedarikte yaşanabilecek darboğazlar, talepte oluşan artışlar/azalışlar ise pazardaki farklı durumlar kısmında karşımıza çıkmaktadır. Tüm bu alanlardaki yapılacak çalışmalar sonucunda, sadece riskler değil fırsatlar da kolaylıkla ortaya konulacaktır. (Goetze, Henselmann:22-23)

Risklerin tespitinde önce konu analizi yapılmaktadır. Bu noktada işletmenin operasyonları sırasında karşılaşabileceği tehlikeler dört unsur yardımıyla incelenmektedir. Bu unsurlar; insan, çevre, yönetim ve kullanılan malzemelerdir. Bu tespitlere göre, işletmede gerçekleşmesi muhtemel olan olası tehlikeler listelenmektedir. Risklere sebep olacak konular da belirlenmektedir. Bu süreçte, birçok risk belirleme tekniği kullanılmaktadır. Bunların arasında; balık kılçığı diyagramı, neden/sonuç analizi, beyin fırtınası analizi, SWOT analizi gibi toplam kalite yönetimi uygulamalarında kullanılan teknikler de mevcuttur. Hangi tekniğin kullanılacağı işletmeden işletmeye değişiklik göstermektedir. Bu tür bir yaklaşım, belirli bir

sorunun veya durumun muhtemel nedenlerinin belirlenmesi, keşfi ve gösterilmesi gerektiğinde kullanılmaktadır. Balık kılçığı diyagramında, oluşabilecek risk sağ tarafa, onu ortaya çıkaran nedenler ise sol tarafa yazılarak gösterilmektedir. Her risk için muhtemel bir dizi ana neden vardır. Genellikle malzeme, insan, makine ve metot bunlar arasında yer almaktadır. (Emhan 2006: 213-214). SWOT analizinde (Strenghts, weakness, opportunities, threats) ise güçlü yanlar, zayıf yanlar, riskler ve fırsatlar bir grafikte değerlendirilmektedir. Bu yöntem birçok konuda özellikle uluslararası işletmelerde kullanılan bir yöntemdir ve işletmelerin hedeflerine daha rahat ulaşabilmesi, operasyonlarını büyüterek geliştirebilmeleri için kullanılan kıymetli bir metodolojidir. Bu metodolojiyle kısa ve uzun vadeli hedeflerin takibi de rahatlıkla yapılabilmektedir. (Uysal 2020: 44-45)

Risklerin doğru tespit edilmesi aşamasında, kontrol listeleri hazırlanması, akış şemaları aracılığıyla süreçlerin takip edilmesi, girdi-çıktı analizleri ile gözden kaçabilecek noktaların belirlenmesi gibi teknikler kullanılabilmektedir. Tüm bunlar aracılığıyla işletmenin güçlü ve zayıf yanları üzerine gidilerek potansiyel tehditler ve olası fırsatlar kolaylıkla ortaya konulabilmektedir. (Goetze, Henselmann:20-21)

Risklerin değerinin, yani olası etkilerinin ve risklerin meydana gelme olasılığının hesaplanması risk değerlendirmesi olarak bilinmektedir. Riskin gerçekleşme olasılığının teamüller ve tecrübeler sonucu kurum kültürünün de katkısıyla belirlenmesi sağlanmaktadır. Kurum kültürünün yanında risklerin gerçekleşmesi halinde ortaya çıkacak etkiliin büyüklüğü ve gerçekleşme olasılıklarının belirlenmesinde çeşitli istatistiki yöntemler, uzman kişilerle yapılacak görüşmeler, anketler gibi farklı araçlar da kullanılabilmektedir. (Akçay, 2011: 34) Bu aşama risklerin ölçülmesi ve değerlendirilmesini de içeren en kapsamlı kısımdır.

Gerçekleşme olasılığı kavramı, çoğunlukla işletmelerde yüzde olarak ifade edilmektedir. Genel kabul gören gerçekleşme olasılığı endeksi aşağıdaki şekilde gösterilmektedir:

- %0-%33 – Düşük olasılık
- %34-%70 – Orta Olasılık
- %70-100 – Yüksek Olasılık

Gerçekleşme ihtimali düşük olan riskler, önceliklendirme de arka sıralarda yer almaktadır. Orta ve yüksek olasılıktaki riskler ise ön sıralarda önceliklendirilmekte ve ehemmiyetle analiz edilmektedir. Bu noktada özellikle yüksek olasılıkta görünen risklerin, işletmenin stratejik planlaması süresince öngörülüp

görülmediği de mutlaka göz önüne alınmalı ve incelenmelidir. Risklerin ve fırsatların stratejik planlama, bütçeleme süreçlerinde yer alması, takip edilmesi, bunlara yönelik önlem planlarının oluşturulması, gerçekleşme ihtimali yüksek olan riskler için muhasebe hesaplarında karşılık ayrılıp ayrılmayacağı gibi konular ciddiyetle ele alınmalıdır. Kendisiyle ilgili karşılık ayrılmış olan riskleri ayrıca kurumsal risk yönetimi sürecinde takip etmeye gerek yoktur.

Risklerin gerçekleşme ihtimaline göre sınıflandırmasını aşağıda görülmektedir:

Tablo 8: Gerçekleşme Olasılığının Sınıflandırılması

Düşük	Gerçekleştiğinde kolayca tolare edilebilecek riskler
Orta	Üzerinde analizler yapılarak gerçekleşmesi engellenebilecek riskler
Yüksek	Kontrolü güç olan ve kabul edip edilmemesi tartışılacak riskler

Kaynak: Yazar tarafından oluşturulmuştur.

Risklerin gerçekleşme ihtimalinin belirlenmesinden sonra etkilerinin ortaya konması/hesaplanması kısmına geçilmektedir. Bu noktada, risklerin doğurabileceği zararlar işletmenin belirlediği ölçüm kriterlerine göre analiz edilmektedir. En sık kullanılan ölçüm kriterlerinden biri, riskin faiz ve vergi öncesi kar açısından değerlendirilmesidir. Bu değerlendirme yapılırken işletmenin stratejik hedefleri, stratejik planlamasındaki veriler gözönüne alınmaktadır. Hesaplamalar yapılırken eldeki en güncel fiili veriler ile önümüzdeki dönemin plan (bütçe) verileri beraber kullanılır.

İşletmelerde risk değerleme süreci, denetçinin finansal tablolarda olabilecek yanlışlıklara istinaden gerçekleştirdiği kontrollerden farklı olarak işletmenin amaçlarını etkileyen risklerin analiz edilip takibini içeren bir prosestir. (Doyrangöl 2001: 52)

Risk değerlemesi sırasında kullanılan analizler, kalitatif (niteleyici), yarı-kantitatif (yarı-niceleyici), kantitatif (niteleyici) veya bunların bir birleşimini ifade eden karma analiz olabilmektedir. Etkili kurumsal risk yönetiminin temeli aslında çok iyi bir risk değerlendirme yani risk analizi adımından geçmektedir. Risk değerlendirme aşaması öncesinde işletmeler kendileri için kritik önemi olan maddi/manevi varlıklarını tespit etme yoluna gidebilirler. Risk analizi adımına gelindiğinde, işletme içinde yapılacak anketler, birebir veya toplu görüşmeler, toplantılar ile bu varlıkların sıkıntılı tarafları belirlenmeli, bunların ne gibi riskler doğurabileceği de seçilecek risk analiz yöntemi ile bulunmalıdır. (Çeliktaş 2018: 502)

Aşağıdaki tabloda risklerin etkilerinin sınıflandırma şeması yer almaktadır:

Tablo 9: Risklerin Etkilerinin Sınıflandırılması

Düşük	Hem yaratacakları etkiye hem de finansal neticelerine kolayca katlanılabilen riskler
Orta	İşletmenin ulaşmak istediği amaçları üzerinde olumsuz etkileri olan riskler. Bu risklerin finansal boyutları da orta-yüksek seviyede olabilir.
Yüksek	İşletmenin hedeflerini, stratejilerini ciddi anlamda tehlikeye sokacak olan riskler. Bu risklerin finansal boyutları da oldukça yüksek düzeyde olacaktır.

Kaynak: Yazar tarafından oluşturulmuştur.

Risklerin değerlendirilmesi aşamasında aşağıdaki sorulara verilen cevapların da etkisiyle çeşitli göstergeler kullanılabilir. Bu noktada cevap verilmesi gereken sorular aşağıda yer almaktadır: (Pickett, 2005:24-25)

- İşletmenin temel performans göstergeleri nelerdir?
- Potansiyel risklerin yukarıdan aşağı tespitinde hangi anahtar göstergeler kullanılabilir?
- İzleme için hangi performans ölçümleri kullanılabilir?
- Performan ölçümüne yönelik hangi verilere ihtiyaç vardır?
- Bilgiler ne sıklıkla toplanmalıdır?
- Veri toplama kriterleri nelerdir?
- Veriler nereden ve nasıl elde edilmelidir?
- Veriler nasıl saklanmalıdır?
- Hangi veri kurtarma mekanizmalarına ihtiyaç vardır?

Risklerin analiz edilmesi aşamasının en son noktası ulaşılan tüm bilgiler ışığında risk matrisinin hazırlanmasıdır. Birçok işletmede risk matrisi en çok kullanılan risk raporlama tekniği olarak da yer alır. Risk matrisi aracılığıyla riskler tek bir tabloda sistematik şekilde görülüp değerlendirilebilmektedir. Risk matrisi üzerinde iki boyutlu olarak risklerin hem gerçekleşme olasılığını hem de potansiyel etkilerini görmek mümkün olmaktadır. Risk matrislerinin kullanımı bu konuda yayınlanan rehberlerde de tavsiye edilmektedir. Yine işletmelerin kendi bünyelerinde oluşturdukları risk yönetimi el kitaplarında da hem önemi hem de hazırlanış şekli anlatılmaktadır.

Risk matrisleri, kurumsal risk yönetiminde basit ama etkili raporlama ve izleme araçlarıdır ve işletmelerde risklerin sistemli, bütünsel olarak takip edilmesini sağlarlar. Risk matrisi kullanımı, hem kurumsal yönetim hem de kurumsal risk yönetimi uygulamalarında ve danışmanlığında yaygın olarak kullanılmaktadır. (Cox, 2008: 498).

Bu matrisler, işletmelerin iş yapış şekilleri, risk yönetimi süreçlerindeki yapılarına göre farklı çarpanlarda hazırlanabilir. En yoğun kullanılan matrisler 3x3, 5x5 şeklinde hazırlanmış olanlarıdır. Sık kullanılan risk matrisine bir örneği yer almaktadır:

RİSKİN ETKİSİ	Yüksek	Orta	Yüksek	
	Orta	Düşük	Orta	Yüksek
	Düşük	Düşük		Orta
		Düşük	Orta	Yüksek
		RİSKİN GERÇEKLEŞME OLASILIĞI		

Şekil 13: Risk ve Fırsat Matrisi

Kaynak: Yazar tarafından oluşturulmuştur.

Yukarıdaki risk matrisinde yatay alanlar riskin gerçekleşme ihtimalini gösterirken, dikey alanlar ise riskin oluşması sonucunda meydana gelecek etkiyi ifade etmektedir. Bu iki alanın kesişim noktaları bize risklerin gruplandırmasını (yüksek, orta, düşük) göstermektedir. Hem etkisi hem de gerçekleşme olasılığı yüksek olan riskler, kabul edilemez risk statüsünde değerlendirilmektedir. Yine hem etkisi hem de gerçekleşme olasılığı düşük olan riskler de kabul edilebilir risk olarak nitelendirilmektedir. Bu iki grubun arasındaki

riskler ise orta düzeyde riskler olarak yer alır. Bu matriste yüksek alanda yer alan riskler çok dikkatli ele alınmalıdır. Gerçekleşme olasılığı yüzdesi ve etkisi dikkatle hesaplanmalı ve bu alanda olduğu işletme için kesin ise ve risklerden kaçınma yoluna gidilmeyecekse, bu konular iç denetçiler tarafından titizlikle denetlenmelidir. Aynı şekilde süreç içinde göreceli olarak daha az ihtimam gösterilmesi gereken alanlar hem etkisi hem de olasılığı düşük olanlardır. İşletmenin bu risklerden zarar görme ihtimali oldukça düşük olarak değerlendirilmelidir. Düşük alandakilerde iş süreçlerinde bazı iyileştirmeler yapılarak bu risklerden kaçınabilme ihtimali olup olmadığı da ayrıca tetkik edilmelidir.

3.3.3.3. Risklerin Önceliklendirilmesi

Risklerin değerlendirilmesi aşamasından hemen sonra önceliklendirilmesi oldukça önemlidir. Önceliklendirme risklerin tiplerine veya olası zararlarına göre yapılabilir. Örneğin yasal mevzuatlara uyum konusunda bir risk öngörüsü varsa bu riske öncelik verilmesi aşikardır. Bu noktada önceliklendirilirken daha önce belirlenmiş olan önem eşikleri de dikkate alınır.

Risk önceliklendirmesi kurumsal risk yönetimi süreci boyunca aralıklarla gözden geçirilmelidir. Çünkü analiz süreci sonrasında elde edilen bilgilere göre önceliklendirmedeki kriterler değişmiş olabilir, dolayısıyla önceliklerin güncellenmesi gerekebilir. Bu noktanın sürecin bu adımında atlanmaması önem arz etmektedir.

3.3.3.4. Risk Cevaplarının Ortaya Çıkarılması & Bütüncül Bakış Açısı Geliştirme (Risk Stratejileri)

Güncel COSO çerçevesinin performans adımında risk değerlemesi sonrası sıra risk cevaplarının oluşturulmasına gelmektedir. Risklerin cevaplanması denildiğinde, kurumsal risk yönetiminin riskler karşısındaki alabileceği aksiyonları ortaya çıkarmak anlaşılmalıdır. Yapılan değerlendirmeler sonucu oluşturulan risk matrisine bakarak ve işletmenin risk iştahı gibi kavramları da göz önüne alarak özellikle etkisi ve gerçekleşme ihtimali yüksek risklere karşılık önlem planları yapılmaya başlanır. İşletmeler riskler karşısında riski azaltma, riskten kaçınma, riski paylaşma, riski kabul edip operasyona devam etmeyi seçebilmektedir. (Usman 2018: 1596-1597).

Genelde işletmeler eğer risk iştahları çok düşük değilse, işletme bünyesinde etkili çalışan bir iç kontrol sistemleri ve dolayısıyla düzgün işleyen kurumsal risk yönetimi sistemleri varsa, bu noktada riskin

verebileceği potansiyel zararları göz önüne alıp yani riski kabul edip operasyonlarına devam etmeyi seçebilirler. Bu noktada genellikle sadece kabul etme stratejisi değil aynı zamanda riski azaltma stratejisi de kullanılır. Bu sayede hem faaliyetlerin devamlılığı sağlanır hem de çeşitli önlem planları yapılarak risk azaltma yoluna gidilir.

Riskten kaçınma stratejisi, işletmelerin belirli faaliyetlerinden vazgeçmeleri anlamını taşıyacağı için çok zor durumda kalınmadıkça tercih edilen bir yöntem değildir. Bazı belli şartların gerçekleşmesi ve riski göze alıp operasyona devam etmenin önü alınamaz riskler barındırması halinde çok dikkatli düşünerek bu karar verilmektedir. İşletmeler bu kararları verirken, sürdürülebilirliklerini tehlikeye atmaktan kaçınmalı, her işletmenin en önemli hedefi olan kazançlarını maksimize etmekten ödün vermemelidir. Ayrıca yatırım yapmaya, işletmenin büyümesine engel teşkil edecek kararların altına imza atmamaya da ehemmiyet göstermelidir.

Üst yönetimin kabul ettiği riskler, sonraki süreçlerde de kurumsal risk yönetimi sürecinde gözlenmeye devam etmelidir. (Marchetti, 2012: 29).

Değerlendirmeler yapılırken daha önce işletmede meydana gelen olumsuz olarak değerlendirilebilecek her olay dikkatle incelenmeli ve bu olayların gelecekte de ortaya çıkıp çıkamayacağına yönelik analizler yapılmalıdır. Bu analizlere atasözümüz "Bir musibet bin nasihattan iyidir." rehberlik edebilir. Bu değerlendirmelerin sonuçlarına göre de risklere yönelik önlem planları yapılır. Risk yönetimi stratejilerinden hangilerinin seçileceği bu hususta çok önemlidir.

Riskin transfer edilmesi seçeneğinde risk başka bir firmayla paylaşılmaktadır. Riskin sigorta edilmesi de bazı risk türlerinde uygulanabilen bir risk stratejisidir. Riskin paylaşılması veya transfer edilmesinde riskin tamamı veya bir kısmı bu stratejiye maruz bırakılabilir. Risk paylaşılırken ortaya maliyet de çıkabilir. Burada işletmeler mutlaka fayda-maliyet analizi yaparak bu kararları vermelidir. (TÜSİAD, 2008: 60-61).

Tüm bu değerlendirmeler sonucunda, işletmeler aşağıdaki stratejilerden biri veya birkaçını seçebilmektedirler:

Tablo 10: Risk Stratejileri

Riskten Kaçınma		Bu yöntem, risk taşıyan faaliyetlerle uğraşmamayı veya riskli işlemleri terk etmeyi içerir. Meydana gelebilecek kötü durumlara karşı şirketlerin veya bireylerin potansiyel tehlikelere karşı alınması gereken önlemleri içermektedir. Örneğin, bir kişi veya kuruluş kendi parasını tehlikeye atmadan mülk satın almak yerine mülk kiralama yolunu seçebilir.
Riski Kabul Etme		İşletmelerin en sık kullandığı tekniktir. Burada önemli olan bu seçeneğin bilinçli şekilde tercih edilmesidir. Eğer işletmeler risk sonucunda meydana gelebilecek durumları hesaplayıp/tahmin ederek kontrol altında tutmaya çalışıyorsa bu teknik sağlıkla uygulanıyor demektir. Meydana gelebilecek risklere karşı plan yapılmış olup çeşitli önlemler geliştiriliyorsa burada aktif kontrol var diyebiliriz Ancak bir işletmede meydana gelebilecek potansiyel tehlikelere karşı herhangi bir işlem yapılmıyorsa yani önlem planları mevcut değilse o zaman pasif kontrolden söz edebiliriz.
Riski Transfer Etme		Burada, işletmenin ilgili riski başka bir işletmeye transferi anlaşılmaktadır. Buna örnek olarak inşaatlarda taşeron kullanımı verilebilir.
Riski Azaltma		İşletmeler, risklerin gerçekleşmesi halinde ortaya çıkabilecek risklerin azaltılmasına yönelik önlemler alınabilir. Örneğin, çeşitli sebeplerle satışlarının azalacağına yönelik riskler olduğu tespit eden işletme bu risklerin hesaplanması ve değerlendirmesini takiben ilgili riskin azaltılmasına yani satışın bir miktarda olsa artırılmasına yönelik indirim verme seçeneği üzerine yoğunlaşarak riski azaltma yöntemini tercih edebilir.
Riskin Sigorta Edilmesi		İşletmelerin bazı riskleri güvence altına almak için kullandığı ve sıklıkla da tercih edilen bir yöntemdir.

Kaynak: Yazar tarafından oluşturulmuştur.

Yukarıdaki tabloda yer alan stratejilerden kendi durumuna uygun olanlarını seçmek ve ilgili alanlarda uygulamak işletmenin sorumluluğundadır. Her işletme için uygun olan stratejiler farklıdır. İşletmeler içinde bulundukları sektör, faaliyet gösterdikleri pazarlar, uluslararası veya yerel bir firma olup olmadıkları,

işletmenin mali durumu gibi birçok faktörü dikkate alarak bu kararı vereceklerdir. Karar verdikleri risk stratejilerine göre kurumsal risk yönetimi sürecinin çıktıları da değişiklik gösterecektir.

COSO 2004'te kontrol faaliyetleri olarak geçen içerik aslında işletmelerin risklere cevap verme aşamasında destek aldıkları işletme içindeki prosedür/yönetmelikleri de ifade etmektedir. En yaygın olarak kullanılan kontrol faaliyetleri içinde üst düzey raporlar, fiziksel kontroller (envanter vb.), performans göstergeleri, görev ve sorumlulukların ayrıştırılması yer alır. Bütün bunlar işletmenin operasyonlarını gerçekleştirebilmesi için, her seviyedeki çalışan tarafından günlük işler esnasında sürekli dikkate alınan mevzuat/prosedürlerdir.

COSO 2017 ile sürecin bu adımında bütüncül yaklaşım getirme ifadesi kullanılmaya başlanmıştır.

İşletme, risklere ve belirsizliklere ilişkin portföy bakış geliştirmekte ve bütüncül değerlendirme yapmaktadır. Portföy bakış açısının farkı, işletmenin strateji ve hedefleriyle ilişkili risklerin ve bunların işletmenin performansı üzerindeki etkilerinin birlikte değerlendirilebilmesidir. (Güler, Arkın 2018:54).

3.3.4. Risklerin Gözden Geçirilmesi

Risklerin incelemeye tabi tutulması ve gözden geçirilmesi, risk yönetimi uygulamalarının güncel ve amaca yönelik olmasını sağlayan önemli adımlardan biridir. Zaman içinde risklerin etkileri ve gerçekleşme olasılıklarını da etkileyen unsurlar, aynı zamanda da bu risklerin yönetiminde oluşabilecek olan maliyetler değişebileceğinden izlemenin devamlı yapılması önem arz etmektedir. (Bozkurt, 2010: 23-24)

Faaliyetler normal akışında devam ederken yapılan doğrulamalar, muhasebe sistemlerinin belli dönemlerde kontrol edilmesi, hesap bakiyelerinin, hesaplarda yapılan işlemlerin tutarlılığının kontrolü, fiziksel mallar ile sistemler üzerindeki malların teyidi gibi faaliyetler, kontrol izleme faaliyetleri arasında yer alır. (Doyrangöl 2002: 34)

Kurumsal risk yönetimi, işletmelere kurulduktan ve etkili bir biçimde çalışmaya başladıktan sonra yapılması gereken en önemli şey sistemin sürekli güncellenmesi, risk izleme sırasında ortaya çıkabilecek sorunlu alanların tespiti ve bunların düzeltilmesi ile sistemin güçlendirilmesidir. Bu şekilde işletmenin performansı artırılabilmekte, hedeflerine ulaşması sağlanmakta, güncel koşullara uyum sağlaması imkanı da mümkün hale gelebilmektedir. (Akçay 2011: 36)

Kurumsal risk yönetimi faaliyetlerinin sıkı bir izlemeye tabi tutulması işlevini etkili şekilde gerçekleştirilebilmesi ve güncel kalabilmesi için şarttır. Bu izleme yapılırken çeşitli varsayımlar, yöntemler, veri kaynakları, analizler dikkate alınmaktadır. (Günbey, 2008: 102) Tün bu belgelerin, düzenli şekilde kayıt altına alınması, saklanması gerekir. Sürecin kayıt altına alınarak belgelenmesinde aşağıdaki iki prensip dikkate alınmalıdır. (TÜSİAD, 2008: 63)

- Yasal ve operasyonel gereksinimler,
- Kayıtların oluşturulması ve saklanmasının maliyeti.

İzleme faaliyetinin sürekliliğinin sağlanması, işletmenin sürekliliğinin sağlanmasına dolaylı olarak katkıda bulunan nihai süreç adımıdır.

3.3.5. Risklerin Raporlanması, İletişimin Sağlanması

Kurumsal risk yönetimi sürecinin bir sonucu olarak risklerin ve fırsatların düzenli olarak ilgili mercilere raporlanması gerekmektedir. Bu noktada günümüzde işletmelerin sürdürülebilirliklerinin ciddi olarak tartışıldığı düşünülürse risk/fırsat raporlamasının şeffaf bir şekilde gerçekleştirilmesi çok önem arz etmektedir.

Kurumsal risk yönetiminin en son konusu bu bilgi ve iletişim alanıdır. Burada işletmenin hesap verebilirliği, güvenilirliği, adilliği, şeffaflığı gündeme gelmektedir. İşletmenin her kademesinde yukarıdan aşağı ve aşağıdan yukarı bilgi aktarımları layıkıyla gerçekleştirilmelidir. Kurumsal risk yönetimine yönelik periyodik raporlama dönemleri olmalı ve bunlar aksatılmamalıdır. Ayrıca işletmenin her biriminde ve her çalışan seviyesinde risk kültürü ve farkındalığının oluşturulması bu noktada en gerekli şeydir. Bir işletmede risk farkındalığı mevcutsa ve çalışanlar kendilerini sorunlu bir alan gördüklerinde bunu ifade etmek anlamında özgür hissediyorlarsa, ellerini taşın altına koymaktan, müdahale etmekten çekinmiyorlarsa biz olması gereken risk kültürünün işletme içinde yerleştirilmiş olduğunu söylenebilmektedir. Bu güvenin çalışanlara verilmesi de yine üst yönetimin sorumluluğu altındadır.

Kurumsal risk yönetimini yalnızca organizasyonel şemalar, standartlar, el kitapları, süreçlerle yönetilememektedir. Kurumsal risk yönetiminde esas olan sürekliliktir. Bu sağlanmadığında her an riskler artmaktadır. Bu süreç ciddi bir eğitimi ve bu işe gönül vermeyi gerektirir. Risk, serseri bir mayın gibi işletmenin her alanında dolaşır, işletmeden bağımsız gibi görünse de ortaya çıktığı anda tüm sistemi çökme

tehlikesi ile karşı kaşıya getirebilir. Bu nedenle işletmelerde oluşturulması gereken en önemli kavram risk farkındalığıdır. Kurumsal risk yönetimi, risk odaklı iç denetim gibi süreçlerin düzgün işlemediği, layıkıyla tesis edilmemiş olduğu işletmeler bir anda iflas edebilir, batma tehlikesi ile karşılaşabilirler. Aslında içinde bulundukları durumun belirtileri işletme mevcut olsa bile, işletmede yönetim kademesinin bu belirtileri görüp risk yönetimi sürecini işletecek derecede farkındalıkları ve bu konuda bilgi&tecrübeleri olmadığında bu son ile karşılaşılabilmektedir. Günümüzde hem küresel dünyada hem de ülkemizde bunun örneklerini maalesef sıklıkla görülmektedir. (Küçüközmen 2012, 66:6)

Bilgilerin ve iletişimin konuşulduğu bir yerde işletmenin kullandığı bilgi sistemlerinden de bahsetmek gerekir. İşletmelerin her bölümlerinde birbiriyle entegre şekilde çalışan, farklı raporlar üretebilen, üzerinde yetkilendirme-onay şemalarının görülüp takip edilebildiği, sıklıkla bilgi-işlem tarafından kontrol edilen, sistem güvenliği açısından testlere tabi tutulan çeşitli sistemler kullanılması günümüz şartlarında kıymetlidir. Mevcut sistemlerin zamanla birlikte güncellenmesi, yenilenmesi, birbiriyle çelişen noktalar varsa tespit edilip düzeltilmesi gereklidir. Burada sistemin kullanıcılarından gelen geri bildirimler de dikkate alınmalıdır.

Bu noktada yine işletmelerde meydana gelen hile, kanuna aykırı işlem vb.uygunsuz operasyonların gerekli mercilere bildirilmesi için kırmızı hat vb. isim lerle oluşturulmuş olan iletişim kanalları olması gereklidir. Çalışanlar, bu hatlara bildirimde bulunduklarında rencide edilmeyeceklerini, sıkıntılı bir duruma düşmeyeceklerini bilmeli ve buna gönülden inanmalıdırlar. Aksi takdirde, bu hatlara bilgi vermekte çekinebilirler. Bu güvenin onlara verilmesi işletmedeki ilgili birimlerin en kıymetli görevlerinden biridir. Günümüzde işletmelerde bu hatlar sıklıkla kullanılmakta ve bu hatlardan gelen bilgiler ile birçok riskli durum tespit edilebilmektedir.

4. İÇ DENETİM ve KURUMSAL RİSK YÖNETİMİNDE İÇ DENETİMİN ROLÜ

4.1. İç Denetime Genel Bakış

Denetim kelimesinin kökeni Latince'deki 'Audire' kelimesinden gelmektedir. Bu kelime, işitme-anlama anlamına gelirken, aslında uzmanların görevli çalışanları dinleyerek yapılan çalışmaları analiz etmeleri ve doğruyu bulmaya çalışmalarını ifade etmektedir. (Cömert, 2016:9)

Denetimin konumu açısından bakıldığında denetçiler; bağımsız denetçi, iç denetçi ve devlet denetçisi olarak üç bölüme ayrılır. İç denetçiler tarafından gerçekleştirilen denetime iç denetim denir. (Cömert, 2016:10-12)

İç Denetim faaliyetlerinin IIA tarafından yapılan tanımı da aşağıdaki şekildedir:

"İç denetim, bir işletmenin faaliyetlerini geliştirmek, onlara değer katmak amacını güden bağımsız ve tarafsız bir güvence ve danışmanlık hizmetidir. İç denetim; işletmenin kontrol ve kurumsal yönetim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik, sistematik ve disiplinli bir yaklaşım geliştirerek kurum hedeflerinin gerçekleştirilmesine yardımcı olur." (Pickett, Pickett 2005: 13)

İç denetimde amaç, işletme varlıklarının her türlü zarara karşı korunup korunmadığı ve tüm işletme faaliyetlerinin ilgili politika/prosedürlere uygun gerçekleştirilip gerçekleştirilmediğinin tespit edilmesidir. (Maliye Hesap Uzm.Derneği 1999: 337)

İç denetimden beklenen yararın gerçekleşebilmesi için tarafsız bir bakış açısı ile ve özgür bir ortamda yapılması en önemli iki şarttır. Tarafsızlık, iç denetçilerin görevlerini titizlikle ve işin kalitesini ön planda tutarak, sonucunu zihninde canlandırmadan yapmaları ile ortaya çıkar. Özgür tutum veya bağımsız anlayış ise iç denetim faaliyetinin tarafsız şekilde yürütülmesinin ön şartıdır. Başkalarının müdahalesi olmadan işini yapabilmek anlamına gelir. Ancak bu şartlar sağlandığında yapılan iç denetimin işletmeye katma değer katacak sonuçlara ulaşabilmesi mümkün olmaktadır. (The Institute of Internal Auditors, 2010).

Günümüzde tüm işletmeler istisnasız iç denetim çalışmalarına ihtiyaç duymaktadırlar. Bu ihtiyacın ana sebepleri aşağıda sıralanmıştır: (Türedi, Karakaya ve İldem, 2011: 66-67)

- İşletmede yöneticilerin ve ilgili tüm çalışanların sorumluluklarını etkili ve verimli bir şekilde yerine getirmelerini özendirir.
- Her seviyedeki çalışanın, işletmenin faaliyetlerinin sonuçlarına yönelik hesap vermesine olanak sağlar.
- İşletme sahiplerinin, hissedarlarının ve üst yöneticilerin işletme kaynaklarını verimli kullanıp kullanmadıkları hususunda analizler yapmalarına imkan verir.
- Yöneticilere danışmanlık hizmeti, çalışanlara ise gerekli durumda eğitim hizmeti sağlar.
- İşletmelerde ortaya çıkabilecek maddi kayıpların saklanmasının önüne geçerek, bunların ortaya çıkarılması ve gerekli düzeltmelerin yapılmasını hatta tekrarlanmaması için önlem alınmasını temin eder.
- İşletme yönetiminde etkili bir rol oynayamayan pay sahiplerinin haklarının korunmasını sağlar.
- Yönetim kadroları ile çalışanlar arasında iletişimi ve koordinasyonu sağlar.
- Tüm personelin hem kendi yaptıkları işlerin sonuçlarını görmelerini hem de işletmeye olan katkılarını fark etmelerini sağlar.
- Dış denetimin daha etkili yapılması ve dolayısıyla daha kısa sürede tamamlanarak bağımsız denetim maliyetinin düşürülmesine katkıda bulunur.

İç denetimin kapsamı içine giren en önemli risk grubu şüphesiz suiistimallerdir. Suiistimaller, işletmeler için hem maddi hem manevi en önemli kayıp nedenidir. Etkili bir iç kontrol sistemi kurularak tüm faaliyetlerde suiistimal olup olmadığının tespiti işletme yöneticilerinin sorumluluğudur. İşletme içerisinde nesnel denetimler yapan iç denetim çalışanları, iç kontrol yapısının etkililiği konusunda güvence vererek sürece ciddi katkıda bulunurlar. İşletmedeki kurumsal risk yönetiminin etkililiğini değerlendirerek suiistimal risklerinin var olup olmadığını da tespit ederler. Burada önemli olan bu tür risklerin ortaya çıkmasını engelleyecek kontrol mekanizmalarının işletmede kurulmuş olmasıdır. İç denetçiler denetim sırasında kritik (kırmızı bayraklı) durumlara dikkat edip, suiistimale yol açabilecek her sorunu tespit etmeli ve raporlamalıdır. Suiistimal ile ilişkili her bildirimde mutlaka ihbar/ iftira kavramlarına azami dikkat gösterilmelidir. Güvenli ihbar hatlarının sağlıklı çalışmasının sağlanması, suiistimal risklerinin en aza indirilmesinde etkili bir araçtır Bu incelemelerde mahremiyet, hız, uzmanlık ve mevzuata uygunluk şartlarına özen gösterilmelidir. (Görmen 2021:102).

Neticede iç denetim faaliyetinin katma değer yaratan bir tarzda gerçekleştirilmesi halinde işletmenin stratejilerine ulaşması yolunda ona destek olduğundan bahsedilebilir. Ancak güncel iş hayatında tabii ki iç

denetim uygulamaları yürütülürken birçok zorluk yaşanmaktadır. Denetlenen bölüm/konuyla ilgili denetimin sonucunda ortaya çıkan tablo ile işletmenin maruz kaldığı maddi zararı, kimi zaman itibar kaybını denetim esnasında öngörebilmek çok kolay değildir. Bu zorluğa ek olarak bir de iç denetim bulgularının işletmeler tarafından ne kadar önemsendiği, verilen önerilerin ne kadar hayata geçirileceği yine farklı tartışma konularıdır. (Baloğlu, Ülker, Adiloğlu 2019: 42) Tüm bunlara rağmen, iç denetim raporunda beyan edilen problemli alanlar ile işletmeye sorunlu alanların düzeltilmesine yönelik verilen öneriler işletme tarafından samimiyetle ve hızlıca analiz edilip gerçekleştirildiğinde iç denetim işletmenin hem hedeflerine ulaşmasına hem de sürdürülebilirliğine katkı sağlar.

İç denetimin ilk kez XIII. yüzyılda İtalya'da ticari işlemlerle ilgili muhasebe kayıtlarının kontrolünde uygulandığı, Amerika Birleşik Devletleri'nde denetçilerin demiryolu şirketlerinin bilet kontrolü ile ilerlediği iddia edilmekle birlikte bu konuya yönelik ilk belgelerin XV. yüzyılda ortaya çıktığı bilinmektedir. 18.yüzyılda ise İngiltere'de Sanayi Devrimi'nin etkisiyle kurulan büyük ölçekli işletmelerin içeriden denetlenme ihtiyacının oluşması ile gelişme göstermiştir. 1930'lu yıllara gelindiğinde, ABD'de Menkul Kıymetler Yasası, Menkul Kıymetler Borsası Yasası yayınlanmış ve yasalarda denetim ve muhasebeye yönelik birçok düzenleme yer almıştır. Ayrıca yine bu dönemde Birleşik Devletler Menkul Kıymetler ve Borsa Komisyonu (SEC) kurulmuştur. Bu yasal düzenlemelerin bir sonucu olarak işletmelerde iç denetim birimleri kurulmaya başlanmıştır. 1941 yılında ise İç Denetçiler Enstitüsü'nün (the Institute of Internal Auditors-IIA) kurulması iç denetimde bir dönüm noktası olarak kabul edilmektedir. Buna mukabil, 1947 senesinde IIA tarafından "İç Denetçilerin Sorumlulukları Bildirgesi" yayımlanmıştır. Bu bildirgede yer alan bilgiler arasında; iç denetimin anlamı, amaçları ve çalışma alanları da yer almaktadır. (Adiloğlu 2011:16)

Tarihi gelişimi içinde iç denetim; 1950 yılı ve öncesinde genelde sadece muhasebe işlemlerinin doğruluğunun test edilmesi şeklinde bir anlam ifade ederken, 1960'larda satıcılara yapılan ödemeler, müşterilerden yapılan tahsilatlar, banka işlemleri gibi işletmenin önemli diğer finansal süreçlerinin denetimini de kapsar hale gelmiştir. (Pickett 2003:10-11) 1970'lerde, 1980'lerde ise ortaya çıkan bazı şirket skandallarının sonucu olarakta iç denetim kıymetli bir meslek haline gelmiştir. ABD'de 1977'de çıkarılan Yolsuzluk ve Rüşvet Önleme Yasası (Foreign Corrupt Practices Act), halka açık şirketler için kurulması gereken iç kontrol sistemine dair önemli hükümler içermekteydi. Bu yasanın en ayırıcı özelliği ise, yasada iç kontrol sistemi sorumluluğunun ilk defa üst yönetime verilmiş olması idi. Yine 70'li yıllarda kurulan Basel Komitesi'nin (Bankacılık Düzenleme ve Denetim Uygulamaları Komitesi-Committee on Banking

Regulations and Supervisory Practices) en baştaki görevi; bankalarda iç denetim faaliyetlerinin düzenlenmesi ve etkililiklerinin artırılması olmuştur. (Ercan, 2008:279)

İç denetim ve ona yönelik tüm kavramların gelişmesine ve bugünkü anlamını kazanmasına en çok katkı yapan kurumlardan biri de The Committee on Sponsoring Organizations of the Treadway Commission (COSO)'dır. COSO tarafından 1992'de yayımlanan ve yıllar sonra 2013'de revize edilen İç Kontrol-Bütünleşik Çerçeve (Internal Control-Integrated Framework) ile 2004'te yayınlanan Kurumsal Risk Yönetimi – Bütünleşik Çerçeve (Enterprise Risk Management-Integrated Framework) iç denetimin rayına oturmasında mihenk taşı olmuştur. İlk yayınlanan raporda, iç denetçilerin rol ve sorumlulukları, etkili bir iç kontrol sisteminde almaları gereken görevler net şekilde vurgulanmıştır. Daha sonra ise, risk yönetimi sürecinin tüm sorumluluğu üst yönetim ve yönetim kurulu üyelerine verilmiş, iç denetçilerin mali işler yöneticileriyle beraber destek görevlerde oldukları belirtilmiştir. İşte bu nokta, iç denetim ve risk yönetimi konularında üst yönetimin kendilerini daha sorumlu görmelerine, işletmelerinde etkili iç kontrol sistemleri ve risk yönetimi sistemlerinin kurulması için çaba harcamalarına neden olmuştur. Yaratılan bu iklim içinde iç denetim işlevleri ciddi anlamda önem kazanmış ve her geçen gün kurumsal risk yönetimi sürecinde iş hayatına bir yenilik ve farkındalık getirebilecek gelişmeler yaşanmaya başlamıştır. (Pehlivanlı, 2014:12)

Bu gelişmeler sonucunda, 2002'de ABD'de de yayınlanan SOX (Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Yasası) gerekli tüm düzenlemeleri içermektedir. Bu yasa aracılığıyla, üst yönetimin ve denetim kurulunun sorumlulukları düzenlenmiş ve bağımsız denetçilerin görevlerine de sınırlamalar getirilmiştir. Bu düzenlemeler aracılığıyla, iç denetim kontrol işlevinden ziyade risk yönetimi işlevini ön plana alan bir hale gelmiştir.

2015 yılına gelindiğinde ise, IIA ilk defa misyon kelimesini kullanarak stratejik yönetime yeni bir bakış açısı kazandırmıştır. Uluslararası Mesleki Uygulamalar Çerçevesi'nin içeriğinde bazı değişikliklere gitmiştir.

Bugünkü anlamda modern iç denetim yani risk odaklı iç denetimin gelişim süreci şu şekilde sıralanabilir:

- 1950-1960-> maddi/manevi varlıkların korunması, bilgilerin güvenilirliğinin güvence altına alınması-Kontrol temelli denetim
- 1970-1980-> uygunluk/mevzuat denetimi-Süreç temelli denetim

- 1980-1990-> işletmenin başarısının denetlenmesi, işletme stratejilerinin gerçekleşmesinin denetlenmesi- Risk temelli denetim
- 2000-günümüz->kurumsal risk odaklı denetimlerin ortaya çıkması-Risk yönetimi temelli denetim

Kontrol temelli denetimde hedef yönetmeliklere ve mevzuata uygunluktur. Odak noktası, uygunluk hatalarının belirlenmesidir. Bu hataların belirlenmesinde uygunluk testleri ve istatistik temelli testler kullanılmaktadır. Süreç temelli denetim de ise, sürecin etkililiği ölçülmektedir. Bu yapılırken mevcut süreç ile olabilecek en iyi süreç karşılaştırılmaktadır. Bu şekilde aradaki boşluklar belirlenerek analiz yapılır. Burada da farklı uygunluk testleri kullanılmaktadır. Risk temelli denetimin hedefi ise, kontrollerin süreçlerin etkililiğine ve risklerin azaltılmasına yönelik katkılarının ölçülmesidir. Önemli risklerin belirlenmesi, değerlendirilmesi burada denetime tabi olur. Bu tespitler çeşitli anlamlılık ve uygunluk testleri ile gerçekleştirilmektedir. Risk yönetimi temelli denetim de ise, amaç işletmenin hedeflerine ve stratejilerine ulaşması yolunda risk yönetimi sürecinin etkililiğinin ölçülmesidir. Bu ölçümün yapılabilmesi için işletmenin hedeflerinin anlaşılması, risk yönetimi adımlarının denetim esnasında tek tek değerlendirilmesi gerekmektedir. (Pehlivanlı, 2014:14-15)

Güncel iç denetim yaklaşımında, risk yönetiminin önemli hale geldiğini ve hatta risk temelli iç denetim kavramının ortaya çıktığı görülmektedir.

4.1.1. İç Denetimin Türkiye'deki Gelişimi

Osmanlı Döneminde 1900'lü yılların başında teftiş birimleri olarak daha çok kamu kurumlarında ve banka gibi kuruluşlarda oluşturulan geleneksel iç denetim, Cumhuriyet döneminde kamu kuruluşlarında ve kamu iktisadi kuruluşlarında, bankalarda, ve sigorta şirketlerinde bugün de aynı isimle ifade edilebilen teftiş kurulu olarak yer almıştır. Doğrudan icrai birimin başındaki kişiye (genel müdüre) bağlı, hata ve hile odaklı ve geçmişe dönük olayları denetleyen müfettişlik kurumu 2001 yılından itibaren özellikle bankalarda ve sigorta kuruluşlarında modern iç denetime evrilmiştir. 2001'de yayınlanan Bankaların İç Denetim ve Risk Yönetim Sistemleri Hakkında Yönetmelik, bu konuda bir milatdır. Bu yönetmelikte Teftiş birimlerinin risk yönetimi ve iç kontrol birimleri ile birlikte iç denetim sistemini oluşturduğu ve teftiş biriminin doğrudan yönetim kuruluna raporlama yapması esasını getirmiştir. [*] Diğer yandan 1999 yılında, Helsinki

[*] Bu konuda ayrıntılı bilgi için bakınız: Gürdoğan Yurtsever, Teftişten İç Denetiem Banka Müfettişliği, Kasım 2009, TBBB, Yayını (E erişim: https://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/KITAP.pdf

zirvesinde Türkiye'nin Avrupa Birliği'ne (AB) aday ülke olarak resmen kabul edilmesinin ardından, mali yönetim ve kontrol alanındaki mevcut yasal düzenlemelerin AB mevzuatıyla uyumlaştırılması yönünde çalışmalar başlamıştır. 2000'li yılların başından itibaren, Uluslararası Para Fonu ve Dünya Bankası ile yürütülen anlaşmalar çerçevesinde, bu alandaki çalışmalar ivme kazanmıştır. Bu çalışmaların sonucunda, kamu kesimi de iç denetim ihtiyacının farkına varmış ve ilk olarak T.C. Merkez Bankası 2002 yılı sonunda İç Denetim Genel Müdürlüğünü kurup faaliyete geçirmiştir. Ardından 24.12.2003 tarih ve 25326 sayılı Resmi Gazetede yayımlanan ve bütün hükümleriyle 01.01.2006 tarihi itibariyle yürürlüğe giren 5018 sayılı "Kamu Mali Yönetim ve Kontrol Kanunu", düzenleyici ve denetleyici kurumlar hariç olmak üzere genel yönetim kapsamındaki kamu kurum ve kuruluşları bünyesinde iç denetimin kurulmasını düzenlemiştir. Söz konusu kanun çerçevesinde, iç denetimin sağlıklı bir şekilde hayata geçirilmesi ve kamu kurum ve kuruluşlarında uygulanabilmesi için gerekli çalışmalar yapılmış ve gerek idari gerekse yasal altyapının oluşturulması noktasında son derece önemli adımlar atılmıştır. (Çevikbaş, 2011,48). Bütün bu gelişmeleri takiben 14 Şubat 2011 tarihli ve 27846 sayılı resmi gazetede yayınlanarak Temmuz 2012 den itibaren yürürlüğe giren 6102 Sayılı Türk Ticaret Kanunu 375. maddesinde, yönetim kurulunun devredilmez ve vazgeçilmez yetkileri arasında muhasebe ve finans denetimi ve şirket yönetiminin gerektirdiği ölçüde, finansal planlama için gerekli düzenin kurulması gerektiği aynı bağlamda , finansal denetim düzeninin kurulması, şirketin işlemlerinin denetlenmesine ilişkin bir iç denetim sisteminin ve ilgili bölümün belirlenmesi hükmüne yer verilmiştir.

Türkiye'de iç denetimin tarihinden bahsederken sivil bir mesleki oluşum olan Türkiye İç Denetim Enstitüsü (TİDE)'den de bahsetmek gerekir. 1995 Yılında 47 kurucu üyenin girişimi ve gayretiyle kurulan Türkiye İç Denetim Enstitüsü aynı yıl İlk Uluslararsı İç Denetim Sempozyumu gerçekleştirdi. Ardından 1996 yılında Uluslararası İç Denetçiler Enstitüsü ve Avrupa İç Denetim Enstitüleri Konfederasyonuna kabul edildi. 2000 yılından itibaren Uluslararası İç Denetçi Sertifikası sınavını ülkemizde yapmaya başladı. .(TİDE, Kilometre Tasları). TİDE bugün ülkemizde modern iç denetimin gelişmesine önemli katkılar sunan, bu amaçla nitelikli yayınlar çıkaran, uluslararası İç Denetim Mesleki Uygulamalar Çerçevesini ve diğer rehberleri Türkçeye çevirerek uygulamada anlaşılmasına katkı sağlayan, aynı bağlamda eğitimler, kongreler, akademik forumlar ve gelecek zirveleri düzenleyen ve iç denetçileri uluslararası geçerli belgelerle sertifikalandıran dernek statüsünde bir sivil kuruluş olup geniş kesimlerce kabul gören bir meslek örgütü olarak görev yapmaktadır

4.1.2. İç Denetim ve Üçlü Savunma Hattı

İç denetimin bir işletmede üzerine alacağı sorumlulukların belirlenmesinde "Üçlü Savunma Hattı Modeli" kullanılır. Birinci savunma hattı operasyonel yönetimdir. Bu ilk hat, etkili iç kontrollerin oluşturulması ve risk/kontrol prosedürlerinin işletme içinde yürütülmesinden sorumludur.

İkinci savunma hattında, operasyonel birimlere dışarıdan destek veren, riskleri kontrol eden ve aslında birinci hattaki kontrollerin meydana gelmesini sağlayan ve takip eden risk yönetimi, mali kontrol, bilgi işlem güvenliği, kalite kontrol, insan kaynakları gibi birimler yer alır. (Özbilger, 2021:41)

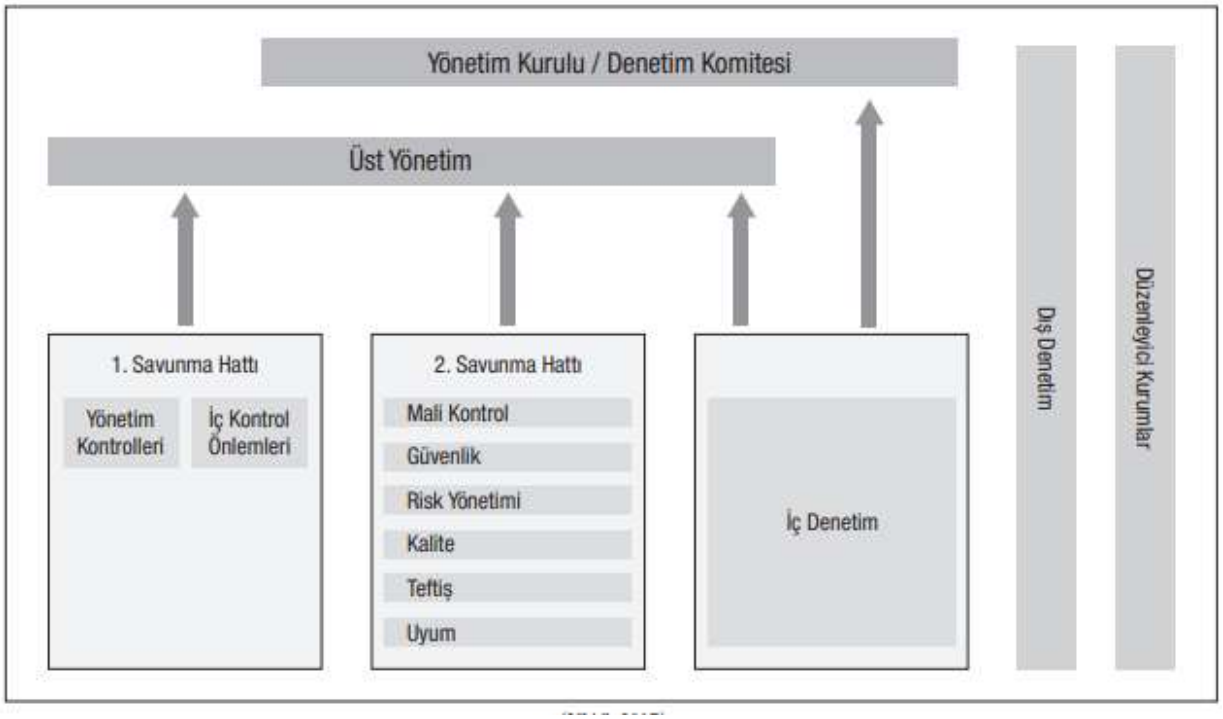
Genelde yönetim fonksiyonlarını içeren bu iki hattan sonra tanımlanan üçüncü hat denetimdir. İç denetim, tahmin edebileceğimiz gibi, birinci ve ikinci savunma hatlarının verimliliğinin değerlendirilmesinden sorumludur (The Institute of Internal Auditors, 2013). İç denetim üzerine düşen sorumluluklardan güvence hizmetlerini işletmenin kurumsal risk yönetimi ve kontrol süreçlerini bağımsız bir değerlendirme yapabilecek kadar nesnel ve detaylı bir şekilde incelemek yolu ile gerçekleşmektedir. Üzerindeki diğer sorumluluk olan danışmanlık hizmetini ise, yol yordam göstermek, önerilerde bulunmak, gerektiğinde farkındalığı artırabilmek için eğitim vermek gibi faaliyetleri yerine getirmek suretiyle gerçekleştirir. (The Institute of Internal Auditors, 2010). İç denetim gibi bağımsız denetim de üçlü savunma hattının üçüncü kademesinde yer alır.

Bağımsız denetim, mali tablolardaki finansal bilgilerin önceden belirlenen ölçütlere uygun şekilde hazırlanıp/sunulup sunulmadığına yönelik değerlendirmelerde bulunan bir denetim türüdür. Bu denetim türünde bağımsız denetçi, denetim sonunda tutarlı ve doğru bir yargıya ulaşabilmek için gerekli olan denetim testlerini uygulamakla yükümlüdür. Bağımsız denetçinin buradaki amacı, işletmelerin kamuoyuna açıkladıkları mali bilgilerin doğru, şeffaf ve gerçeğe uygun olduklarının denetim yoluyla saptanması, denetim raporunun hazırlanması ve dolayısıyla işletmenin tüm paydaşları nezdinde makul bir güvence yaratılmasıdır. Bağımsız denetim sürecinde, işletmenin iç kontrol süreci ile muhasebe sistemleri incelenir, hatalar veya eksik noktalar belirlenir. (Özyiğit, Yıldırım 2022: 368). Neticede bağımsız denetim de iç denetim gibi işletmenin süreçlerinin iyileştirilmesi için çok kıymetlidir ve işletmeye bu süreç için kritik önemde veriler sunar.

Kurumsal risk yönetimi odaklı bağımsız denetim denildiğinde ise, işletmenin kaynaklarının adil ve doğru şekilde kullanılması ile hedeflerin gerçekleştiği, başarılı bir mali raporlamanın gerçekleşmesi için

işletmedeki tüm risklerin değerlendirilip takip edilmesini içeren bir süreç anlaşılmaktadır. Bağımsız denetim de iç denetim gibi kurulum aşamasında kurumsal risk yönetimine danışmanlık hizmeti verir, sonrasında da kurumsal risk yönetiminin Bağımsız denetim sürecinin, işletmelere ve paydaşlarına sağladığı faydalar da göz önüne alındığında, etkili bir kurumsal risk yönetimi sisteminin oluşturulması sırasında bağımsız denetim öncelikli faaliyetler arasında yer alır. (Özyiğit, Yıldırım 2022: 369). Tüm bu sebeplerden ötürü bağımsız denetim üçlü savunma hattının son aşamasında kritik öneme sahip bir fonksiyondur.

Üçlü savunma hattının ilgili kademelerindeki kişiler/birimler aşağıdaki tabloda gösterilmiştir.



Şekil 14. Üçlü Savunma Hattı

Kaynak: ECIIA, FERMA işbirliği ile hazırlanan "AB Şirketler Hukuku 8.Yönergesi (Madde 41) için kılavuz dokümandan alınmıştır.

Üçlü savunma modeli, kolay anlaşılır olmasına ve otoriteler tarafından kabul görmesine rağmen bazı olumsuzluklara sebep olmuştur. Burada soruna yol açan ana mevzu, modelin tasarımı değil daha çok modelin uygulanma şekli olmuştur. Uygulamada yaşanılan aksaklıkların başlıca nedenlerine aşağıda yer verilmiştir:

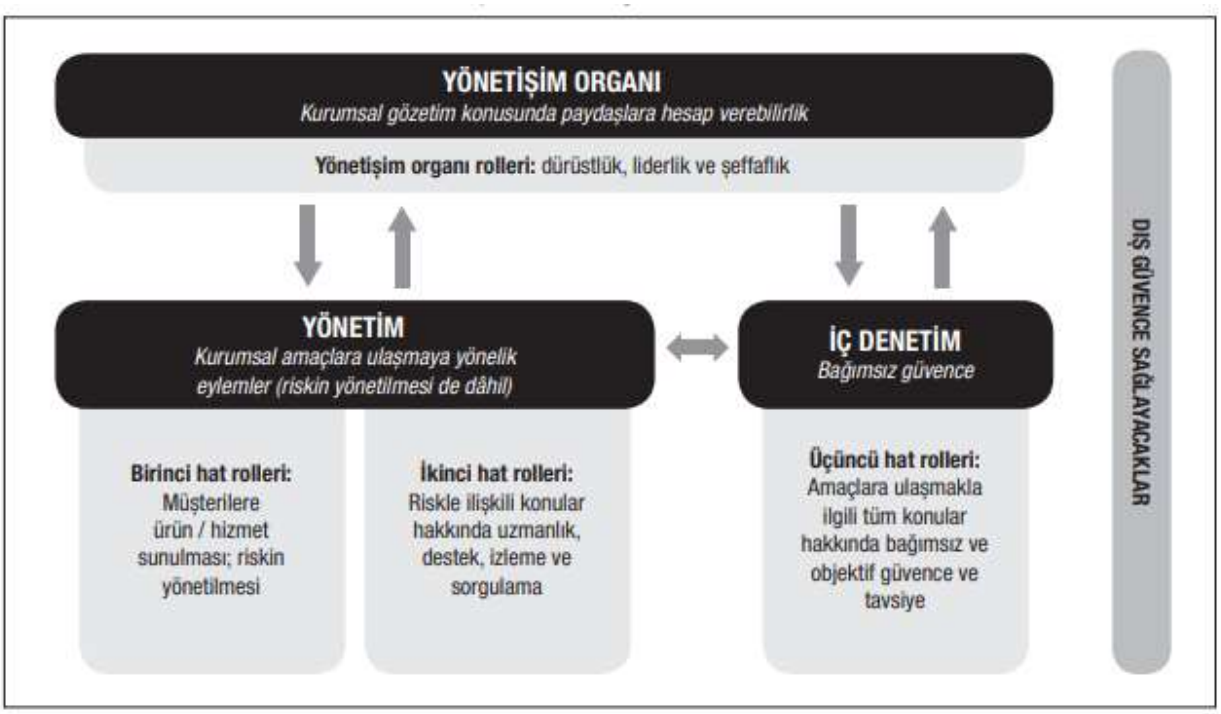
- Üçlü savunma hattında roller ve sorumluluklar şekil üstünde kolay anlaşılır olmasına rağmen modelin çalışması sırasında bazı kafa karışıklıkları meydana gelmiştir. Bu soruna genellikle hatlar arasındaki ilişkilerin çizgilerinin net çizilmemiş olması sebep olmuştur.
- Hatların zaman zaman iç içe geçen görevleri sebebiyle aralarında bir koordinasyon sorunu ortaya çıkmıştır.
- Birinci ve ikinci hattaki kişilerin aynı işletme içinde görevli olması ancak farklı hatlarda yer almaları birlik duygusuna zarar vermiş, aralarındaki iletişimde sıkıntılar olmuştur. (Özbilger, 2021:43-44)

Yukarıdaki nedenlerin sonucu olarak, Uluslararası İç Denetçiler Enstitüsü harekete geçip modelin güncellenmesini sağlamış ve Üç Hatlı Model ismiyle kullanıma sunmuştur. (IAA, 2020)

IAA tarafından geliştirilen Üç Hatlı Model'de hedef, koordinasyon ve işbirliğinin yatay olarak sağlanması ve modelde yer alan tüm pozisyonların kendi arasında entegre şekilde çalışmasının garanti altına alınmasıdır. Bu noktada hat mantığı ardışık gelen süreçleri ifade etmemekte, eşzamanlılık içermektedir. (Burca, 2020) Yeni modelin önceki modelden farklı olan yanları aşağıda gösterilmiştir:

- Müdafaa anlamına gelen savunma kelimesi modelin isminden çıkarılmıştır. Burada amaç savunmayı ortaya çıkarmak değil proaktif davranışı ön plana çıkarmaktır.
- Yeni modelde altı adet ilke benimsenmiştir. Bunlar yönetişim, yönetişim organının rolleri, yönetim, birinci ve ikinci hatların rolleri, üçüncü hattın rolleri, üçüncü hattın bağımsızlığı, değer yaratma ve korumadır. (Özbilger, 2021:45)
- Eski model ile kıyaslandığında roller ve sorumluluklar net şekilde belirlenmiştir.

Aşağıdaki tabloda hatlar ve sorumluluklar net şekilde görülmektedir.



Şekil 15: Üçlü Hat Modeli

Kaynak: IIA,2020.

4.2. Uluslararası İç Denetim Mesleki Uygulama Standartları (2017 ve öncesi)

İç denetim standartları, ilk olarak 1978'de yayınlanmış ve zaman içinde ihtiyaçlara binaen güncellenmiştir. Bu standartlar, denetimin uygulanmasına yönelik bir çerçeve oluşturur ve ülkelere göre de bazı farklılıklar içerebilir. Standartlarda iç denetimin mesleki uygulaması ve uygulamanın etkililiğinin değerlendirilmesine dair ihtiyaçlar ile kullanılan terimlerin açıklamaları da yer almaktadır.

İç denetim faaliyetleri doğal olarak farklı hukuki ortamlarda ve yine farklı büyüklükte olan, farklı sektörlerde faaliyet gösteren işletmelerde işin uzmanları tarafından gerçekleştirilmektedir. Tüm bu farklılıklar tabii ki uygulamaları etkilemektedir. Ancak burada önemli olan iç denetim çalışmasının Uluslararası İç Denetim Meslekî Uygulama, Standartları'na uyumlu şekilde ve sorumluluk bilinci olan iç denetçiler tarafından gerçekleştirilmesidir.

Standartların genel amaçları aşağıdaki şekilde sıralanabilir:

- İç denetim uygulamasını ifade eden temel ilkeleri tanımlamak.
- İç denetim faaliyetlerinin etkililiğini ve yaratacağı katma değeri desteklemeye yönelik bir çerçeve sağlamak.
- İç denetim performansının doğru şekilde değerlendirilmesine uygun bir ortam yaratmak.
- Gelişmiş kurumsal süreç ve faaliyetleri artırmak/teşvik etmek

Standartlar, etik kurallar ile birlikte, uluslararası mesleki uygulama çerçevesi'nin tüm zorunlu unsurlarını kapsamaktadır. (TİDE, 2017:1)

IPPF uyarınca iç denetim ilkeleri aşağıda yer almaktadır:

- Yetkililik ve mesleki özen sergiler.
- Tarafsızdır ve bağımsızdır
- İşletmenin stratejileri, hedefleri ve riskleri ile uyumludur.
- Kaliteli ve sürekli gelişmekte olduğunu gösterir
- Etkili bir iletişim kurar.
- Risk temelli güvence sağlar.
- Algılaması güçlü, proaktif ve gelecek odaklıdır.
- Örgütsel gelişimi teşvik eder.

İç denetimde meslek ahlakı yani etik kurallar çerçevesinde mevcut ilkeler, dürüstlük, tarafsızlık, sır saklama ve yetkililiktir. İç denetçiler dürüstlük kavramı çerçevesinde, çalışmalarını doğruluk, dikkat ve sorumluluk duygusuyla yaparlar. Hukuku gözeterek yasa dışı bir faaliyete kendi bilgisi dahilinde taraf olmaz, kendi mesleği çerçevesinde yüz kızartıcı eyleme kalkışmaz. İç denetçiler, tarafsızlıklarına zarar verecek her hangi bir faaliyete katılmaz ve görevleri boyunca elde ettikleri bilgileri korur, saklar, kendi menfaati için kullanmaz.

Şu an yürürlükte olan iç denetim standartları Ekim 2016'da yayınlanmış ve 1 Ocak 2017 itibariyle de yürürlüğe girmiştir.

İç denetim standartları, genel olarak nitelik standartları ve performans standartları olarak ikiye ayrılmıştır. Nitelik Standartlarında, iç denetimin gerçekleştiği işletmelere veya ilgili iç denetçilere yönelik alanlar yer almaktadır. Performans Standartlarında ise iç denetimin temel noktaları ve bu faaliyetin değerlendirilmesine yönelik kalite ölçütleri yer almaktadır. Uygulama Standartları ise tamamlayıcı olarak, güvence veya danışmanlık faaliyetlerine uygulanabilecek gereklilikleri belirterek süreç içinde yerini alır.

Burada güvence hizmetleri; iç denetçinin, bir işletme, süreç, bölüm, sisteme yönelik bağımsız görüşünü sunabilmek için, eldeki tüm bilgi/belgeleri nesnel bir şekilde değerlendirmesini içerir. Güvence hizmetinin içeriğini iç denetçi belirler. Bu hizmetlerin, genelde üç tarafı vardır: Bir işletmede sürecin doğrudan muhatabı olan kişiler (süreç sahipleri), değerlendirmeyi yapacak olan iç denetçiler, değerlendirmeyi kullanan kişiler.

Danışmanlık hizmetleri ise, tavsiye niteliğinde olup görevlendirmeyi talep eden birimin talebi ile gerçekleşmektedir. Bu hizmetlerin içeriği de değerlendirmeyi talep edenler ile iç denetçi arasındaki sözleşmeyle belirlenir. Burada dikkat edilmesi gereken en önemli husus, iç denetçinin danışmanlık hizmeti verirken, nesnel bakışını korumalı ve hiçbir şekilde idarî sorumluluk almamasıdır. Tüm iç denetçiler uluslararası muhasebe standartlarına uymak ile yükümlüdür. (TİDE, 2017:2)

İç denetim standartları genel olarak iki ayrımda incelenebilir. Birincisi Nitelik standartlarıdır. Nitelik standartlarının özetini aşağıdaki tabloda görebilirsiniz.

Tablo 11. Nitelik Standartları

Nitelik Standartları	
Amaç, Yetki, Sorumluluklar	Zorunlu Rehberin İç Denetim Yönetmeliğinde Tanınması
Bağımsızlık ve Objektiflik	Kurum İçi Bağımsızlık Yönetim Kurulu İle Doğrudan Etkileşim İç Denetim Yöneticisinin İç Denetim Haricindeki Görevler Bireysel Objektiflik Bağımsızlık veya Objektifliğin Bozulması
Yeterlilik ve Azamî Meslekî Özen ve Dikkat	Yeterlilik Azamî Meslekî Özen ve Dikkat Sürekli Meslekî Gelişim
Kalite Güvence ve Geliştirme Programı	Kalite Güvence ve Geliştirme Programının Gereklilikleri İç Değerlendirmeler Dış Değerlendirmeler Kalite Güvence ve Geliştirme Programı Hakkında Raporlama "Uluslararası İç Denetim Meslekî Uygulama Standartlarına Uygundur" İbaresinin Kullanılması Aykırılıkların Açıklanması

Kaynak: Yazar tarafından oluşturulmuştur.

Amaç, yetki, sorumluluklar: İç denetim yönetmeliğinde iç denetimin amacı ve iç denetçilerin yetki, sorumlulukları açıkça yer almalıdır. İşletmeye sunulan güvence ve danışmanlık hizmetinin niteliği yönetmelikte tanımlanmak zorundadır. İç denetimin mesleğinin temel prensipleri, ilgili etik kurallar, standartlar ve iç denetimin tanımına uyma mecburiyeti iç denetim yönetmeliğinde tanınmak zorundadır. (TİDE, 2017:4)

Bağımsızlık ve Tarafsızlık: İç denetim çalışması mutlaka bağımsız olmalıdır ve iç denetçiler de görevlerini yaparken nesnel davranmak mecburiyetindedir.

Bağımsızlığın gerçekleşebilmesi için, iç denetim yöneticisi üst yönetime ve yönetim kuruluna doğrudan ve sınırsız biçimde ulaşma olanağına sahip olmalıdır. Bağımsızlık düsturunu tehlike altına sokabilecek

konular, mutlaka ilgili kişiler tarafından doğru seviyede ele alınmalıdır. Tarafsızlık ise iç denetçinin görevini, denetim sonucunda ortaya çıkan bulgulara tamamen inanacağı ve savunacağı şekilde denetimin kalitesinden taviz vermeden yapmasını sağlayan tutumlar bütünüdür. Burada önemli olan iç denetçinin kendi yargılarına ve ulaştığı sonuçlara göre davranabilmesidir. Ayrıca işletme içinde, iç denetçiler sağlıklı bir çalışma yürütebilecekleri bir kademeye bağlı olmalıdırlar ve yılda en az bir kez yönetim kuruluna iç denetim faaliyetinin bağımsızlığını teyit etmelidirler. Bu noktada iç denetim bütçe ve kaynak planlarının onaylanması, yönetimle ilgili iç denetim kapsamı ve mevcut ise sıkıntılı konulara yönelik görüşmelerin yapılması gibi konular önem kazanır.

İç denetim yöneticisi, işletmede yönetim kurulu ile doğrudan iletişimde olmak zorundadır. İç denetim yöneticisinin görevinin dışında kalan bazı sorumlulukları var ise ya da işletmede böyle bir beklenti varsa, bağımsızlık ve tarafsızlığının yıpranmasını engelleyecek tedbirlerin alınması gerekir. Yönetim kurulu bu noktada gözetim faaliyetini yerine getirerek tedbir alabilir. İç denetçiler, tarafsız ve önyargısız biçimde davranmak ve her türlü menfaat çatışmasından kaçınmak zorundadır.

Denetçilerin bağımsızlığı/nesnelliğinin fiilen bozulduğu veya bozulduğu izlenimi doğduğu takdirde, bozulmanın ayrıntıları ilgili taraflara açıklanmak zorundadır. (TİDE, 2017:5-6)

Yeterlilik ve Azamî Meslekî Özen ve Dikkat: İç denetimde görevlerin, mesleki yeterlilik ve azamî özen ile yerine getirilmesi zorunluluğu vardır.

İç denetçiler, görevlerini yerine getirmek için gereken bilgi, becerilere sahip olmalıdır. Bu nedenle, iç denetçiler, Uluslararası İç Denetçiler Enstitüsü (IIA) ve diğer ilgili meslekî kuruluşlar tarafından verilen Uluslararası İç Denetçi (CIA) unvanı ve diğer unvanlar gibi uygun meslekî unvan sertifikalarını alarak alandaki yeterliliklerini ispatlamak için teşvik edilirler. (TİDE, 2017:7)

İç denetçiler ne kadar mesleki özen gösterirse göstersin bazen risklerin tamamını öngörememiş olabilirler.

İç denetçiler danışmanlık görevi sırasında, görevin sonuçlarının kapsamı, zamanlaması, raporlanması da dahil olmak üzere kendilerinden beklenen tüm talepleri karşılamalıdırlar. Ayrıca iç denetçiler, mevcut bilgi ve becerilerini her geçen gün artırabilmeleri için düzenli olarak meslekî gelişimlerine yatırım yapmalıdırlar. (TİDE, 2017:7)

Kalite Güvence ve Geliştirme Programı: İç denetim yöneticisi, iç denetim faaliyetini her yönüyle kapsayan bir kalite güvence ve geliştirme programı hazırlayıp bu programı uygulamakla yükümlüdür. Sözkonusu programın oluşturulmasının amacı, iç denetim faaliyetinin standartlara uygun şekilde değerlendirilmesini mümkün kılmaktır. Ayrıca bu program vasıtasıyla iç denetim faaliyetinin verimliliği de değerlendirilir. Bu programda hem iç hem de dış değerlendirmeler yer almalıdır. İç değerlendirmeler; iç denetim faaliyetinin performansının devamlı izlenmesini sağlar. Devamlı izleme, iç denetim faaliyetinin gözetimi, gözden geçirilmesinin kıymetli bir parçasıdır. Dış değerlendirmeler ise, işletme dışından konuya vakıf ve bağımsız bir değerlendirme uzmanı veya ekibi tarafından en az beş yılda bir yapılmak zorundadır.

İç denetim yöneticisi, uygulanan kalite güvence ve geliştirme programının neticelerini mutlaka üst yönetime ve yönetim kuruluna aktarmak zorundadır. (TİDE, 2017:10-11)

Nitelik standartlarından sonra performans standartlarını da özet olarak aşağıdaki tabloda görebiliriz:

Tablo 12. Performans Standartları

Performans Standartları	
İç Denetim Faaliyetinin Yönetimi	Planlama Bildirim ve Onay Kaynak Yönetimi Politika ve Prosedürler Koordinasyon ve İtimat Üst Yönetim ve Yönetim Kuruluna Raporlamalar Dış Hizmet Sağlayıcı ve Kurumsal Sorumluluk
İşin Niteliği	Yönetişim/Kurumsal Yönetim Risk Yönetimi Kontrol
Görev Planlaması	Planlamada Dikkate Alınması Gerekenler Görev Amaçları Görev Kapsamı Görev Kaynaklarının Tahsisi Görev İş Programı
Görevin Yapılması	Bilgilerin Tespiti ve Tanımlanması Analiz ve Değerlendirme Bilgilerin Kayıtlı Hâle Getirilmesi Görevin Gözetim ve Kontrolü
Sonuçların Raporlanması	Raporlama Kıstasları Raporlamaların Kalitesi Hata ve Eksiklikler "Uluslararası İç Denetim Mesleki Uygulama Standartları'na Uygun Olarak Yapılmıştır" İbaresinin Kullanılması Görevlendirmelerde Aykırılıkların Açıklanması Sonuçların Dağıtımı Genel Görüşler
İlerlemenin Gözlenmesi **Risklerin Kabul Edildiğinin İletilmesi**	

Kaynak: Yazar tarafından oluşturulmuştur.

İç Denetim Faaliyetinin Yönetimi: İç denetçiler denetim faaliyetini, işletmeye katma değer yaratacak şekilde yönetmek zorundadır. Bir iç denetim, iç denetim yönetmeliğinde mevcut olan amaçlara ulaştığında, standartlara uygun şekilde gerçekleştirildiğinde, işletmenin etkilenebileceği tüm durumlar dikkate alındığında etkili şekilde uygulanmış demektir. İç denetim faaliyeti, işletmenin stratejileri, hedefleri ve riskleri dikkate aldığında işletmeye değer katar; yönetişim, risk yönetimi süreçlerini geliştirmek için alternatif yollar önermek için uğraşır ve nesnel olarak bunlarla ilgili güvence sağlar. (TİDE, 2017:12)

İç denetim yöneticisi, işletmenin hedeflerine uygun olarak, iç denetim faaliyetinin önceliklerini de belirleyen risk esaslı plan yapmak mecburiyetindedir. Bu planı hazırlarken üst yönetim aracılığıyla işletmenin risk yönetimi süreçlerine hakim olunur ve sonrasında plan nihai hale gelir. Süreçlerde değişiklik olması durumunda bu planda değişiklik gösterebilir. İç denetim faaliyetinin görev planı, en az yılda bir kez yapılan yazılı bir risk değerlendirmesine dayanır. Üst yönetim, denetim komitesi ve yönetim kurulu, bu sürece mutlaka dahil edilmektedir. İç denetim yöneticisi, görevinin risk yönetimini geliştirme, katma değer yaratma kısımlarını da düşünerek teklif edilmesi halinde danışmanlık görevlerini kabul etmeyi düşünmelidir ve kabul edildiğinde denetim planına da dâhil edilmelidir. Sözkonusu plan üst yönetim, denetim komitesi, yönetim kurulu tarafından onaylanmalıdır. Onaylanmış planın uygulanabilmesi için, iç denetim kaynaklarının uygun ve yeterli olmasını ve etkili bir şekilde kullanılmasını sağlamak iç denetimin görevidir.

İç denetim faaliyetinde göz önüne alınacak olan politika ve prosedürlerin şekli ve içeriği, iç denetim faaliyetinin büyüklüğüne, yapısına göre değişiklik gösterir. (TİDE, 2017:13)

Denetim esnasında aynı çalışmaların gereksiz yere tekrarlanmasını engellemek, denetimin kapsamını doğru belirleyebilmek için diğer iç ve dış güvence ve danışmanlık hizmeti sağlayıcılarıyla mevcut bilgileri paylaşmalı, koordine olmalı ve onların işlerine güvenmeyi değerlendirmelidir.

İç denetim faaliyetinin amacı, yetkileri, sorumlulukları ve plana kıyasla performansı konularında ve standartlara uyumu konusunda, yönetim kuruluna dönemsel olarak raporlar sunulmalıdır. Bu raporlar, suiistimal risklerini, kurumsal yönetim sorunlarını ve üst yönetimin dikkatini çekebilecek başka konuların da dâhil olduğu önemli riskleri içermelidir. (TİDE, 2017:14)

İşin Niteliği: İç denetim faaliyeti; sistematik ve risk esaslı bir yaklaşımla, işletmenin kurumsal yönetim, risk yönetimi ve kontrol süreçlerini değerlendirmek ve ayrıca bu süreçlerin iyileştirilmesine katkıda

bulunmak durumundadır. Denetçiler proaktif olduklarında, yaptıkları değerlendirmeler yeni anlayışlar sunduğunda ve olası gelecek etkileri göz önünde bulundurduklarında iç denetimin güvenilirliği ve değeri artmaktadır.

İşletmenin hedefleri misyonunu destekliyorsa, önemli riskler belirlenmişse ve analiz edilmişse, işletmenin risk iştahına uygun risk cevapları uygulanmaya konulduysa, risk yönetimine yönelik gerekli raporlamalar ilgili kişilere ve sıklıkla yapıldıysa o işletmede risk yönetimi süreçlerinin etkili olduğuna dair iç denetçide bir kanı oluşabilir. (TİDE, 2017:15-16)

Risk yönetimine ek olarak, iç denetim faaliyeti suiistimalin gerçekleşme ihtimalini ve işletmenin bu konuya dair riskini nasıl yönettiğini de değerlendirmek zorundadır. İç denetçiler, danışmanlık görevleri sırasında elde ettikleri risklere yönelik bilgileri, işletmenin risk yönetim süreçlerini değerlendirmede kullanmak zorundadır. İç denetçiler, risk yönetim süreçlerini kurmada veya geliştirmede yönetime yardım edebilir ancak bu noktada riskleri yönetme sorumluluğunu almaktan kaçınmalıdırlar.

İç denetim faaliyeti, işletmedeki kontrollerin verimliliğini değerlendirmek ve aynı zamanda sürekli gelişimi teşvik etmek suretiyle, işletmenin etkili kontrollere sahip olmasına destek olmak durumundadır. İç denetçiler, danışmanlık görevleri sırasında elde ettikleri kontrol bilgilerini işletmenin kontrol süreçlerini değerlendirmek için kullanmak zorundadır. (TİDE, 2017:16-17)

Görev Planlaması: İç denetçiler, her bir görev için amaç, kapsam, zamanlama ve kaynak dağılımına yönelik yazılı bir plan hazırlamak zorundadır. Bu planı hazırlarken iç denetçiler denetlenecek işletmenin stratejileri, hedefleri, kontrol süreçleri, mevcut riskleri, risklerin kabul edilebilir düzeyde tutulabilmesi için yapılması gerekenleri, kurumsal yönetim, risk yönetimi sürecinin, kontrol süreçlerinin etkililiğini ve gelişme olanaklarını dikkate almalıdır.

Görevin kapsamı, görevin amaçlarını karşılayacak seviyede olmalı ve güvence görevi sırasında önemli bir danışmanlık fırsatı çıkarsa, görevin amacı, kapsamı, karşılıklı sorumluluklar, beklentiler üzerine yazılı bir anlaşma hazırlanmalı ve danışmanlığın neticeleri standartlara uygun olarak raporlanmalıdır.

İç denetçiler, görev amaçlarına ulaşacak iş programları hazırlamak ve bunları yazılı hâle getirmek zorundadırlar. İş programları, görev sırasında uygulanacak bilgi toplama, analiz, değerlendirme gibi noktaları içermeli ve görev başlamadan önce onaylanmalıdır.

İç denetçiler, üzerlerine aldıkları görevdeki hedefe ulaşmak için yeterli bilgileri tespit etmek, analiz etmek, değerlendirmek zorundadır. Güvenilir bilgi, uygun teknikler kullanılarak elde edilen bilgidir (TİDE, 2017:17-18)

İç denetçiler, vardıkları kanaatleri ve sonuçlarını uygun değerlendirmelere dayandırmak zorundadır.

İç denetçiler, denetim sonuçlarına dayanak teşkil eden yeterli, güvenilir ve faydalı bilgileri kayıtlı hale getirmek zorundadır. İç denetim yöneticisi, tüm bu kayıtlara erişimi kontrol etmek zorundadır ve gerektiğinde, bu kayıtları işletme dışındaki taraflara vermeden önce, üst yönetimin/hukuk danışmanının onayını almak zorundadır. (TİDE, 2017:19-20)

İç denetim görevinin amacına ulaşmasını, kalitenin güvence altına alınmasını ve personelin geliştirilmesini sağlayacak şekilde denetim sürecinin gözetlenmesi ve kontrol edilmesi mecburidir. İç denetim yöneticisinin gözetlenme ve kontrol edilme hususunda sorumluluğu vardır. Gözetim ve kontrole dair uygun deliller, kayıtlı hale getirilip korumaya alınmaktadır. Daha sonra iç denetçiler, görev sonuçlarını raporlamak zorundadır. Bu raporlarda, iç denetimin uygulanabilir sonuçları, tavsiyeleri ve/veya aksiyon planları da yer almak zorundadır. Uygun olan yerlerde iç denetçinin görüşü de sağlanmalıdır. Görüş üst yönetim, kurul ve diğer paydaşların beklentilerini dikkate almak ve yeterli, güvenilir, ilgili ve yararlı bilgi ile desteklenmek zorundadır. Hazırlanan raporlar, doğru, objektif, açık, yapıcı, eksiksiz olmalı ve zamanında sunulmalıdır Nihaî raporlamada önemli bir hata olduysa, iç denetim yöneticisi, hatalı ve eksik raporu alan bütün taraflara düzeltilmiş bilgileri iletmek durumundadır. Etik kurallara veya standartlara aykırılık söz konusu olduysa, raporlama sırasında uygunluğun tam sağlanamadığı ve bu noktanın denetiç sonuçlarına etkisi mutlaka raporda belirtilmelidir. (TİDE, 2017:21)

Denetim neticesinde genel görüş yayınlanırken, işletmenin stratejileri, hedefleri ve riskleri ve üst yönetim, yönetim kurulu ve diğer paydaşların beklentilerinin göz önüne alınması mecburidir. Olumsuz bir genel görüş var ise mutlaka nedenleri açıklanmalıdır.

İç denetim yöneticisi, hem güvence hem danışmanlık hizmetinin neticesinde yapılanları gözlemek zorundadır. Alınması gereken tedbirlerin alınıp alınmadığı, önlem planlarının yapılıp takip edilip edilmediği gözetilmelidir.

4.3. Global İç Denetim Standartları (2024)

2020 yılından beri yoğun bir şekilde standartların yenilenmesine yönelik çalışmalar devam etmiştir ve neticede IIA Standartlar Kurulu, ilgili tarafların görüşlerini de alarak yeni uluslararası iç denetim standartlarını 9 Ocak 2024'te yayınlamıştır ve bu standartlar 9 Ocak 2025 itibariyle yürürlüğe girecektir. Yukarıda detaylı şekilde anlatılan ve 2017 yılında yürürlüğe giren standartlar ise bir yıllık geçiş dönemi süresince kullanılmaya devam edecektir.

Yeni standartta öncelikle standartların adı değişmiştir. Standardın ismi, eskiden "Uluslararası İç Denetim Mesleki Standartları" (The International Standards for the Professional Practice of Internal Auditing) iken yeni yapıda Global İç Denetim Standartları" (The Global Internal Audit Standards) olarak ifade edilmektedir. İsim değişikliği ile başlayan süreç, Uluslararası Mesleki Uygulama Çerçevesi'nin (UMUÇ-The International Professional Practices Framework, **IPPF**) değişmesi ile devam etmiştir.

2017 yılındaki standartta mevcut olan UMUÇ ile 2024 yılındaki güncellemede yer alan UMUÇ'un karşılaştırması aşağıda yer almaktadır:

Şekil 16. 2017 ve 2024 UMUÇ Karşılaştırması

Kaynak: IPPF, 2024.

2017 yılındaki standartta yer alan UMUÇ, aşağıdaki altı unsurdan oluşuyordu. Bu altı unsurdan ilk dördü zorunlu rehber kapsamında, diğer ikisi tavsiye edilen rehber kapsamında idi.

1. İç Denetim Mesleki Uygulaması İçin Ana Prensipler (Core Principles)
2. İç Denetimin Tanımı (Definition)
3. Etik Kurallar (Code of Ethics)
4. Standartlar (Standards)
5. İç Denetimin Misyonu (Mission)
6. Uygulama Rehberleri ve Tamamlayıcı Rehberler (İmplementtion Guidance and Suplemental Guidance)

2024 yılındaki standartta yer alan UMUÇ ise üç unsurdan oluşmaktadır:

1. Global İç Denetim Standartları (Global Internal Audit Standards)
2. Konuyla İlgili Gereklilikler (Topical Requirements)
3. Global Rehber (Global Guidance)

Yeni UMUÇ'ta da şu an kullanılan versiyonda olduğu gibi, "zorunlu" ve "tavsiye edilen" şekilde bir ayrım mevcuttur. Yeni UMUÇ'un "Global İç Denetim Standartları" ve "Konuyla İlgili Gereklilikler" kısmı UMUÇ'un zorunlu iki unsurunu oluştururken "Global Rehberler" ise zorunlu olmayan unsurunu oluşturmaktadır.

2024'te UMUÇ'u oluşturan yeni unsurlardan Global İç Denetim Standartları, küresel olarak iç denetim uygulamalarına rehberlik etmeyi amaçlamakta ve iç denetim birimlerinin kalitesini değerlendirip yükseltmeye yönelik baz oluşturmaktadır. Toplamda 15 adet iç denetim prensibi mevcuttur ve bunlardan her biri kendisini destekleyen gereklilikleri içeren standartlar, uygulamaya ilişkin hususlar ve uyumla ilgili deliller ile desteklenmiştir. (IIA, 2024)

Konuyla İlgili Gereklilikler (Topical Requirements) kısmında ise, risk teşkil eden alanlarda iç denetim hizmetlerinin kalitesini ve tutarlılığını artırmak için iç denetçileri desteklemeye yönelik belgeler yer almaktadır. Bu noktada, denetim planları bu gerekliliklerde belirtilen hususlara riayet ederek hazırlanmalıdır. Konuyla ilgili gereklilikler, değişken risk ortamlarında iç denetimin katma değer yaratmayı

sürdürmesini sağlamayı amaçlamıştır. Konuyla İlgili Gereklilikler alanı da UMUÇ'un bir parçası olarak Standartlar gibi zorunlu unsurlardandır. Öneri değildir.

Global Rehber (Global Guidance) tarafında ise, iç denetim hizmetlerinin gerçekleştirilmesinde zorunlu olmayan ama bilgi ve tavsiye içerikli uygulamaları yer almaktadır. Global Uygulama Rehberleri ve Global Teknoloji Denetim Rehberleri de (GTAG) bu rehberler arasındadır. Bu rehberlere uyulması zorunlu değil, tavsiye niteliğindedir.

Yukarıdaki görüldüğü gibi, yeni UMUÇ'ta zorunlu unsur dört tek bir çatı altında toplanmıştır.

Yeni yapıda, Global İç Denetim Standartları aşağıdaki resimde de ifade edildiği üzere beş ana bölümden oluşmaktadır: (IIA, 2024)

Şekil 17: Global İç Denetim Standartları (2024) Genel Çerçevesi

Kaynak: IPPF, 2024.

Yeni standartlardaki bu beş bölümden "İç Denetimin Amacı" ve "İç Denetim Fonksiyonunun Yönetişimi" kısmı tamamen yeni oluşturulmuştur, "Etik ve Profesyonellik", "İç Denetim Fonksiyonunu Yönetme" ve

“İç Denetim Hizmetlerinin Yürütülmesi” daha önceki versiyonda da mevcut olan bazı kısımların birleştirilmesi ve onlara ekler yapılmasıyla ortaya çıkarılmıştır.

Ayrıca, eski versiyonda mevcut standartlar “nitelik” ve “performans” standartları olmak üzere ikiye ayrılıyordu ve bu standartların altında ilgili standarda ilişkin güvence veya danışmanlık hizmetine yönelik gerekliliklerde Uygulama Standartları içinde yer alıyordu.Yeni versiyonda bu yapı tamamen değiştirilmiştir. Nitelik ve performans ayrımı yapılmamış; güvence, danışmanlık çeşitlendirmesi de standartların içine yedirilmiş durumda verilmiştir. Ayrıca daha önce olan Yorumlar kısmı da 2024’te mevcut değildir.

Yeni yapıda her alanın altında, o alanla ilgili öncelikle genel bilgiler verilmekte, ondan sonra da o alanla ilgili “Prensipler” yer almaktadır. Prensiplerin altında ise, o prensiple ilgili Standartlar ve ilgili Standardın “Gereklilikleri” (Requirements) bulunmaktadır. Bu Gerekliliklerden sonra, “Uygulamaya İlişkin Hususlar” ve bu standartlarla ilgili “Uygunluk Kanıtına İlişkin Hususlar” kısmı (Considiration for Implementation and Evidence of Conformance) da gelmektedir. (Burca, 2024)

Yeni yapıda mevcut olan 5 bölümün altında yer alan 15 prensibi ve bunlarla ilgili standartları aşağıdaki görebiliriz:

Tablo 13: Global İç Denetim Standartları'nın Yapısı (2024)

1.BÖLÜM: İÇ DENETİMİN AMACI	**3.BÖLÜM: İÇ DENETİM FONKSİYONUNUN YÖNETİŞİMİ**
2.BÖLÜM: ETİK VE PROFESYONELLİK	**6.Prensip: Yönetim Kurulundan Alınan Yetki**
1.Prensip: Dürüstlük Göstermek	Standart 6.1: İç Denetimin Görev Tanımı
Standart 1.1: Doğruluk ve Mesleki Cesaret	Standart 6.2: İç Denetim Yönetmeliği
Standart 1.2: Kurumun Etik Beklentileri	Standart 6.3: Yönetim Kurulunun ve Yönetimin Desteği
Standart 1.3: Yasal ve Profesyonel Davranış	**7. Prensip: Bağımsız Konumlandırma**
2. Prensip: Objektifliği Sürdürmek	Standart 7.1: Kurumsal Bağımsızlık
Standart 2.1: Bireysel Objektiflik	Standart 7.2: İç Denetim Yöneticisinin Nitelikleri
Standart 2.2: Objektifliği Koruma	**8. Prensip: Yönetim Kurulunun Gözetimi**
Standart 2.3: Objektifliğe İlişkin Bozulmaların Açıklanması	Standart 8.1: Yönetim Kuruluyla Etkileşim
3.Prensip: Yetkinlik Göstermek	Standart 8.2: Kaynaklar
Standart 3.1: Yetkinlik	Standart 8.3: Kalite
Standart 3.2: Sürekli Mesleki Gelişim	Standart 8.4: Dış Kalite Değerlendirmesi
4.Prensip: Azami Mesleki Özen Göstermek	
Standart 4.1: Global İç Denetim Standartlarına Uyum	
Standart 4.2: Gerekli Profesyonel Özen	
Standart 4.3: Profesyonel Şüphecilik	
5. Prensip: Gizliliği Korumak	
Standart 5.1: Bilgilerin Kullanımı	
Standart 5.2: Bilgilerin Korunması	

4. BÖLÜM: İÇ DENETİM FONKSİYONUNUN YÖNETİMİ	5. BÖLÜM: İÇ DENETİM HİZMETLERİNİN YÜRÜTÜLMESİ
9.Prensip: Stratejik Planlama	**13. Prensip: Görevlerin Etkin Bir Şekilde Planlanması**
Standart 9.1: Yönetişim, Risk Yönetimi ve Kontrol Süreçlerini Anlamak	Standart 13.1: Görevle İlgili İletişimler
Standart 9.2: İç Denetim Stratejisi	Standart 13.2: Görev Risk Değerlendirmesi
Standart 9.3: Metodolojiler	Standart 13.3: Görev Amaçları ve Kapsamı
Standart 9.4: İç Denetim Planı	Standart 13.4: Değerlendirme Kriterleri
Standart 9.5: Koordinasyon ve İtimat	Standart 13.5: Görev Kaynakları
10. Prensip: Kaynakların Yönetimi	Standart 13.6: Görev Çalışma Programı
Standart 10.1: Mali Kaynakların Yönetimi	**14. Prensip: Görev Çalışmalarının Yürütülmesi**
Standart 10.2: İnsan Kaynakları Yönetimi	Standart 14.1: Analiz ve Değerlendirme İçin Bilgi Toplama
Standart 10.3: Teknolojik Kaynaklar	Standart 14.2: Analizler ve Potansiyel Görev Bulguları
11. Prensip: Etkili İletişim Kurmak	Standart 14.3: Bulguların Değerlendirilmesi
Standart 11.1: Paydaşlarla İletişim ve İlişki Kurmak	Standart 14.4: Tavsiyeler ve Eylem Planları
Standart 11.2: Etkin İletişim	Standart 14.5: Görev Sonuçları
Standart 11.3: Sonuçların Bildirilmesi	Standart 14.6: Görevlerin Kayıt Altına Alınması
Standart 11.4: Hatalar ve İhmaller	**15.Prensip: Görev Sonuçların Raporlanması ve Eylem Planlarının İzlenmesi**
Standart 11.5: Risklerin Kabul Edildiğinin İletişimi	Standart 15.1: Görev Nihai İletişimi
12.Prensip: Kaliteyi Artırmak	Standart 15.2: Eylem Planlarının ya da Önerilerin Uygulandığının Teyit Edilmesi
Standart 12.1: İç Kalite Değerlendirmesi	
Standart 12.2: Performans Ölçümü	
Standart 12.3: Görev Performansının Gözetimi ve İyileştirilmesi	

Kaynak: Burca, 2024.

4.4. İç Denetçinin Organizasyondaki Yeri

IIA'in de ifade ettiği üzere; iç denetimin amacı, bir işletmede yöneticilerin görevlerini etkili bir biçimde gerçekleştirmelerine yardımcı olmaktır. Bu bağlamda, bir iç denetçi işletmenin operasyonlarının bağımsız olarak incelemekte ve yönetime bu konuda bilgi vermektedir. Bu şekilde onlara tavsiyelerden bulunarak danısmanlık yapmakta ve degerlendirmelerini aktarmaktadır.

İç denetçiler, işletme içinde iç denetim hizmetini gerçekleştirmeleri için isletme tarafından istihdam edilmis kisilerdir. Bir isletmenin sürekli çalısanı oldukları için ücretleri de isletme tarafından karşılanmaktadır.(Ergin, 2006:15)

İç denetçi, denetlediği faaliyetlerden bağımsız olmalıdır. Yine görev kapsamının belirlenmesi, görevlerini yerine getirmesi ve alınan sonuçların raporlanması aşamalarında her türlü müdahaleden uzak olmalıdır. Aynı zamanda, iç denetçilerin işlerini etkili ve verimli şekilde yapabilmeleri için üst yönetim tarafından desteklenmesi gerekmektedir.

IIA uygulama önerilerindeki ideal yapıya göre, iç denetim birimi yöneticisi, fonksiyonel olarak denetim komitesi ve yönetim kuruluna bağlı ve sorumlu olmalı, idari olarak ise işletmenin başkanına raporlamalıdır.

İç denetim fonksiyonun işletme içindeki yerine bakabilmek için öncelikle iç denetimin en önemli 3 fonksiyonunu hatırlamak gerekir. Bunlar; iç denetimin bağımsızlığı ve tarafsızlığının sağlanması, güvence ve danışmanlık hizmetinde bulunulması ve işletme faaliyetlerini geliştirilmesidir. Denetçinin bağımsız şekilde çalışabilmesi, kendini özgür hissetmesi ve karşılaştığı olaylara tarafsız yaklaşabilmesi ile organizasyondaki yeri arasında önemli bir bağlantı mevcuttur. (Sakin 2017: 68-69)

İç denetçinin güvence hizmeti olarak verdiği hizmetin içeriği, işletmenin kendi politika/prosedürlerine uyup uymadığının tespit edilmesi ve performans kriterlerine uygun şekilde işletmenin yönetilip yönetilmediğinin belirlenmesidir. Buradaki güvence pek tabii ki mutlak değildir. Çünkü bir iç denetçinin mevcut tüm işlemleri tek tek kontrol etmesi işin doğası gereği mümkün değildir. İç denetçi, iç denetim faaliyetinin mevcut standartlara uygun şekilde yerine getirerek mümkün mertebe en yüksek seviyede güvence vermeyi hedeflemektedir.

İç denetçinin diğer önemli işlevi danışmanlık faaliyetidir. Bu faaliyet kapsamında üst yönetime işletmenin mevcut politikalarının, prosedürlerinin, yönetmeliklerinin geliştirilmesine yönelik olarak destek olmak iç

denetçinin bu hususstaki görevlerinden biridir. Burada iç denetçinin işletmeye katma değer yaratma misyonu ile çalışması beklenen ve hedeflenen noktadır. Burada iç deneticinin yönetim kademesine işletmenin kendi stratejilerine katkıda bulunacak önerilerde bulunma, olası riskleri öngörüp bunları fark etmeye yönelik olarak gerekli iç kontrollerin geliştirilmesine destek olma konusunda destek olması beklenmektedir. (Sakin 2017: 70)

İç denetçilerin yukarıda da değinilen görevlerini yerine getirebilmeleri için öncelikle bağımsız olmaları ve görevlerini tarafsız bir şekilde yürütmeleri gerekir. Uluslararası iç denetim standartlarında da bağımsızlık konusuna defaatle yer verilmiştir. İç denetçilerden kendi görüşlerini, yargılarını, düşüncelerini oluştururken bağımsız olmaya çalışmaları, kendilerini kısıtlamamaları istenmektedir.

İç denetçilerin güvence ve danışmanlık hizmetini layıkıyla yerine getirebilmeleri için, iç denetim bölümünün iç denetim komitesine veya doğrudan yönetim kuruluna raporlama yapması tercih edilmelidir. İç denetim ekibinin görevleri rahatlıkla yerine getirebilmeleri için ihtiyaç duydukları yetkilere de sahip olmaları gerekmektedir. Üst yönetimin iç denetçilerin erişmesi gereken her türlü bilgi ve belge için iç denetim ekibine güvence vermesi ve bu hususta aksaklık yaşanmaması için gerekli tedbirleri alması da çok önemlidir. Organizasyondaki yeri bu şekilde belirlenen ve gerekli yetkilerle donatılmış olan iç denetçiler, görevlerini bağımsız, şeffaf, hesap verebilme anlayışı içinde yerine getirebilmektedirler. (Sakin 2017: 71-72)

İç denetim biriminin işletme içinde oluşturulmasında işletmenin büyüklük ölçeği, faaliyet gösterdiği sektör, uluslararası yapıda olup olmaması vb.birçok nokta dikkate alınacaktır. Özellikle holding niteliğinde büyük işletmelerde en büyük işletmenin veya ana şirketin konumlandığı yerde iç denetim biriminin oluşturulması ve oradan diğer işletmelere hizmet verilmesi daha az maliyetli ve uygulaması daha kolay bir çözüm olabilir. İç denetçilerin tek bir yerde konumlanmasının aralarında bilgi paylaşımının daha kolay olması, denetimlerin yürütülmesinde tek bir anlayışın hakim olması açısından birçok avantajı da bulunmaktadır.

4.5. İç Denetçinin Yetki ve Sorumlulukları

İç denetçi ve yönetim kurulu/denetim komitesi arasındaki işlevsel sorumluluk çerçevesinde yer alan görevler aşağıda yer almaktadır:

- İç denetim birimi yönetmeliğini onaylamak,

- Yıllık denetim planını ve bu planda yapılan bütün önemli değişiklikleri incelemek ve onaylamak
- İç denetim risk değerlendirmeleri ve ilgili denetim planını onaylamak
- İç denetim birimi yöneticisi ile, yönetimin bulunmadığı özel toplantılar yapmak, iç denetim faaliyetlerinin sonuçları hakkında raporlar almak, ayrıca iç denetim birimi yöneticisinin gerekli gördüğü diğer konularda raporlar almak.
- İç denetim yöneticisinin atanması veya azli ile ilgili tüm kararları onaylamak
- İç denetim yöneticisinin yıllık ücretinin ve denetim ücretlerinin düzenlenmesini onaylamak
- İç denetim bütçesinin onaylamak, iç denetim faaliyetinin sorumluluk ve görevlerini yerine getirmesine engel olan kapsam veya bütçe kısıtlamaları olup olmadığını tespit etmek amacıyla, iç denetim yöneticisi ve işletme yönetimi nezdinde uygun inceleme ve araştırmaları yapmak
- İç denetim biriminin performansını yılda en az bir kere incelemek

İç denetçinin idari olarak raporlama yaptığı CEO vb üst yöneticiyle olan sorumluluk ilişkisi içinde de, bütçeleme ve yönetim muhasebesi, personel değerlendirmeleri ve ücretleri de dahil insan kaynakları yönetimi, iç haberleşme ve bilgi iletişim konuları yer almaktadır.

İç denetim yöneticisinin, işletmenin kontrol ve gözetim işlevleri kapsamında risk yönetimi, mevzuata uygunluk birimi, etik, çevre ve bağımsız denetim gibi birimlerle ilişkileri de göz önüne alınmalı ve değerlendirilmelidir.

4.6. İç Denetçide Bulunması Gereken Özellikler

İç denetçilerin sahip olması gereken yyetkinlikleri üç ana başlıkta incelemek mümkündür. (Bailey, 2020)

Bunlar,

- Genel yetkinlikler
- Davranışsal beceriler
- Teknik beceriler

Genel yetkinlikler kapsamında, problem çözme becerileri, iletişim becerileri, mevzut veya standartlarıdaki değişiklikleri takip etme ve organizasyonel beceriler gelmektedir.

Davranışsal beceriler ise, etik hassasiyeti, tarafsızlık, takım oyuncusu olabilme yer alır.

Teknik beceriler arasında da işi anlama, veri toplama ve değerlendirme teknikleri, bilgi işlem sistemlerini kullanabilme, iş süreçlerinin analizi, proje yönetimi ve adli suçlara yönelik farkındalık yer almaktadır.

İç denetçiler yukarıdaki yetkinlik listesine göre,

- Problemleri tanıyıp onları çözebilecek dereede b ilgi, beceri ve tecrübeye sahip olmalıdırlar.
- İç denetim uygulamaları esnasında her seviyeden çalışan /yönetici ile yazılı ve sözlü kaliteli iletşim kurabilmeleri gerekir.
- İç denetim, iç kontrol, risk yönetimi kavramları ve bu kavramlara yönelik tüm standart ve uygulamalar hakkında bilgi sahibi olmalı ve bu alanlardaki değişiklikleri önemle takip etmelidirler.
- Etik yönetmelikler/kurallar hakkında yeterli bilgiye sahip olmalı ve bu konuda hassas davranmaları, gizliliğe önem vermeleri gerekmektedir.
- İç denetim süresince nesnel, tarafsız bakış açılarını muhafaza etmeleri gereklidir.
- İç denetim işlevini yürüteceği konuyla ilgili uzman seviyesinde bilgi sahibi olmaları gerekmetedir. Yönetim bilişim sistemlerine ilişkin onları rahatlıkla kullanabilecek oranda bilgi seviyesinde olmaları gereklidir.
- Denetim sürecinde edinilecek verileri toplayabilecek, analiz edebilecek, süzebilecek ve gerekli tüm raporlamaları yapabilecek, sonuçları sunabilecek biçimde veri analizi tekniklerine hakim olmaları gerekmektedir.
- Tüm denetim sürecinin etkili şekilde yürütülebilmesi için müzakere becerileri, sunum becerileri, verimli dinleme teknikleri, stres yönetimi gibi konularda eğitimli ve bilgi olmaları önemlidir.

4.7. Risk Odaklı ve Risk Yönetimi Odaklı İç Denetim Yaklaşımı

İç denetim anlayışının zaman içinde aldığı yol oldukça dikkat çekicidir. Yukarıda ilgili bölümde de bahsedildiği üzere, iç Denetim zaman içindeki evrimini aşağıdaki sıralamada görebiliriz: (Pickett, 2005:144)

- Kontrol bazlı denetim
- Süreç bazlı denetim
- Risk odaklı denetim
- Risk yönetimi odaklı denetim

Kontrol bazlı denetimde genellikle varlıkların korunması sözkonusu iken süreç bazlı denetimde işin içine uygunluk ve mevzuat denetimleri de dahil olmuştur. 1990'lı yıllarda risk odaklı denetime geçildiğinde kontrollerin süreçlerin etkililiğine ve risklerin azaltılmasına yönelik katkılarının ölçülmesi de artık denetim kapsamı içeriğinde yer amıştır. Günümüzde uygulanan risk yönetimi odaklı denetim de ise, amaç işletmenin hedeflerine ve stratejilerine ulaşması yolunda risk yönetimi sürecinin etkililiğinin ölçülmesidir.

Son dönemlerde iç denetim, klasik anlamdaki kontrol odaklı yaklaşımdan uzaklaşmış ve kurumsal risk yönetimi ve dolayısıyla işletmelere değer katmayı esas alan, merkezine stratejilerin geliştirilmesine destek olmayı ve risk belirlemeyi koyan bir yöne doğru gitmiştir. Artık günümüzde iç denetçiler sadece kontrol faaliyetlerini denetlemekle kalmıyor aynı zamanda risklerin tanılanmasını sağlayıp işletmenin risk haritasını sürekli izleyerek kurumsal risk yönetim süreçlerini desteklemektedirler. (Lindow, Race 2002: 29)

Günümüzde kurumsal risk yönetiminin öneminin artması ve işletmelerin başarısındaki rolünün daha iyi anlaşılmasıyla iç denetimin risklere bakış açısı değişmiş ve iç denetçilerin işletmeye daha çok değer yaratabilmesine imkan sağlamak amacıyla risk odaklı iç denetim anlayışının ortaya çıkması sağlanmıştır. Risk odaklı iç denetim ilk olarak ABD'de benimsenmiş ve her geçen gün yaşanan olaylar çerçevesinde gelişmiştir. Risk odaklı iç denetim; kaynakların bir sonunun olduğu, dikkatli kullanılması gerektiği, denetlenecek operasyonel faaliyetlerin farklı risk türleriyle karşı karşıya olduğu ve buralarda karşılaşılan her riskin önem derecesinin de farklı olacağı kabulüne dayanmaktadır. (Kara, Yereli 2012: 68-69)

Risk odaklı iç denetim, denetim kaynaklarının kısıtlı olduğu, denetlenecek çeşitli faaliyetlerin farklı risk türleri ile karşı karşıya olduğu, denetlenecek faaliyetlerin çeşitli düzeyde önem derecelerine sahip olduğu varsayımına dayanan bir denetimdir.(Görener 2010: 32) Risk odaklı iç denetimin amacı, kurumsal risk yönetim sistemlerinin ve iç denetimin planlı ve düzgün çalışıp çalışmadığı, işletmenin hedeflerine uygun şekilde yürüyüp yürümediği ile ilgilenmek ve aynı zamanda yönetim kuruluna bağımsız güvence sağlamaktır. Bağımsız güvence teminatı verilirken şu hususlara dikkat edilmelidir:

- Yönetim tarafından kurumsal risk yönetim süreçlerinin olması gerektiği gibi (eksiksiz, tutarlı) yürütüldüğü
- Yönetim tarafından riskleri kabul edilebilir bir düzeye indirmek amacıyla risklere karşı alınmış önlemlerin yeterli ve etkili olduğu

- Yönetim tarafından kontrol altına alınan risklere karşı oluşturulan önlemler ilgili güvenilir ve uyumlu bir kontrol çerçevesinin uygulanmakta olduğudur. (Türedi, Gürbüz 2015:12)

Risk odaklı denetim süreci, yıllık denetim planlarının risk odaklı olarak gerçekleştirilmesi demektir. Denetlenecek süreçlerin tespit edilip, işletmenin risk haritasının çıkarılması ve kaynakların en riskli faaliyetlerden başlanarak planlanması gerekir. İç denetimin bu noktada önemli görevlerinden biri, işletmenin içinde olduğu rekabet ortamı, yasal mevzuat hükümleri ve işletmenin faaliyet alanındaki güçlü ve zayıf yanları da dahil olmak üzere bir çok faktörü göz önüne alarak, kilit süreçlerde olası risk ve fırsatları belirlemek yer almaktadır. (Keskin 2010:42)

Risk odaklı iç denetim süreci, işletmenin risk profilinin oluşturulması için risklerin belirlenmesiyle başlar, akabinde riskleri sınıflandırmakta ve çeşitli önlemlerle kabul edilebilir seviyeye indirilmesini içermektedir. Risk düzeylerine uygun denetim planları hazırlanıp denetim faaliyetlerine geçilmekte ve neticede tüm bulgular değerlendirilerek raporlanmaktadır. (Akkaya 2011: 81).

Risk odaklı denetimden zamanla kendisini risk yönetimi odaklı iç denetime bırakmıştır. Bu denetimi ise şu şekilde tanımlayabiliriz.(Pickett, 2005:143-144)

- Risk odaklı denetimin sadece işletme hedeflerine, işletmenin riski kaldırma kapasitesine, performans göstergelerine biraz daha odaklanmış halidir.
- Risk odaklı denetim genelde risklerin dayanılabilecek seviyelere indirilmesini amaçlarken, risk yönetimi temelli denetim ise işletmenin hedeflerine ulaşabilmesi için ana risklerin/fırsatların optimize edilmesini de içerir.

Yukarıdaki noktalardan anlaşıldığı üzere, başarılı bir kurumsal risk yönetimi sisteminin en önemli parçası risk yönetimi odaklı iç denetimdir.

Risk yönetimini temeline almış iç denetim faaliyetleri sadece geçmişte yapılmış olan hataları/suiistimalleri/ hileleri tespit etme odaklı değil, gelecekte işletmenin daha iyi yönetilmesi amacıyla risk odaklı yapılmaktadır (ISMMMO 2015: 39).

4.8. Geleneksel İç Denetim ile Risk Odaklı İç Denetimin Karşılaştırılması

Geleneksel iç denetim ile risk odaklı iç denetimin karşılaştırılmasını aşağıda bir tablo ile gösterebiliriz:

Tablo 14. Geleneksel İç Denetim ile Risk Odaklı İç Denetimin Karşılaştırılması

Değerlendirme Alanları	**Geleneksel**	**Risk Odaklı**
İç denetimin ana konusu	İç kontrol	Risk
Denetim yöntemi	Reaktif	Proaktif
Risk değerleme	Faktörler	Senaryolar
Testler	Kontrol odaklı	Risk odaklı
Öneriler	Etkin fayda-maliyet analizi yapılmış mı?	Risk stratejileri doğru tesxpit edilmiş mi?

Kaynak: Kishali, Pehlivanlı 2006:82.

Her iki denetim türünde de risk temel alanı oluşturmakla birlikte, geleneksel denetim doğal risk, kontrol riski ve ortaya çıkartma risklerine odaklanmaktayken; risk odaklı iç denetim, denetim kökenli olmayan daha çok işletme kökenli risklerle de ilgilenmektedir. Geleneksel iç denetimde, iç denetçi çoğunlukla planlama, teknik ve iç kontrolle ilgili ayrıntılarla uğraşarak zamanını harcarken, risk odaklı iç denetimde iç denetçi, işletme süreçlerini anlama ve bu riskleri yönetme üzerine çalışmaktadır. Aynı zamanda geleneksel denetim yönteminde denetçi olmuş bitmiş konuların kontrolüne vakit harcayacağı için yaratacağı katma değer pek fazla olamamaktadır. (Kishali, Pehlivanlı 2006:82) Risk odaklı iç denetimde ise, denetçiler işletmenin kurumsal risk yönetimi süreçleri, süreç içinde tespit edilen riskler üzerinden giderek hem işletmenin stratejilerini gerçekleştirmesi, hedeflerine ulaşmasına hem de işletmede düzenli olarak katma değer yaratılmasına olanak sağlamaktadırlar.

İç denetim, kurumsal yönetimin temel prensiplerinden olması sebebiyle de işletmelerde kurumsal risk yönetimi, kontrol ve kurumsal yönetim süreçleri ile ilgili bağımsız ve tarafsız güvence sağlama ve danışmanlık hizmeti vererek, yönetsel hesap verebilirliğin yerleşmesine destek olmaktadır. İç denetçiler, işletmelere aslında ayna tutarak, işletme körlüğü sebebiyle fark edilmeyen birçok riski teşhis ederek çözüm

yolları aranmasını sağlamaktadır. Tüm bu görevleriyle iç denetim, risk yönetimi ve iç kontrol açısından anahtar rol oynamaktadır. (Akçay 2011: 39)

4.9. Risk Odaklı İç Denetimin Gerekliliği ve İşleyişi

Risk odaklı iç denetimde iç denetçiler iç kontrol ve kurumsal risk yönetim yapılarının tasarımının olması gerektiği gibi olup olmadığını, işletmenin hedeflerine ulaşabilmesi ve stratejilerini gerçekleştirebilmesi için gerekli çalışmaların yapılıp yapılmadığını denetleme amacındadırlar. Kurulan kurumsal risk yönetimi adımlarının ne kadar etkilili olduğunun denetimini de iç denetçiler yaparlar.

Risk odaklı iç denetim anlayışında sadece mali tablo riskleri değil tüm işletme riskleri detaylı denetime tabi tutulmaktadır. Bu şekilde hem kurumsal risk yönetiminin hem de onun bir parçası olduğu iç kontrol sisteminin etkililiği kontrol edilmiş olmaktadır. (Türedi, Zor, Gürbüz,2015: 13-14)

Risk odaklı bir iç denetim yaklaşımının temelinde risklerin başarılı şekilde yönetilmesine destek olmak gelir. İşletmelerin ulaşılabilir hedefler belirleyip belirlemediği, kendilerinin doğru stratejiler geliştirip geliştirmediği de irdelenmektedir. Bu aşamadan sonra ise, işletmelerin hedeflerine ulaşma yolunda karşılaştıkları riskleri nasıl değerlendirdikleri de analiz edilmektedir. İç denetim birimi, detaylı şekilde risk haritasında mevcut olan tüm risklerin sınıflandırılmasını, yani türlerine göre ayrılma sürecini, gerçekleşme olasılığı ve etkisinin nasıl tespit edildiğini, kabul edilen riskler için alınan önlemleri ve bunların uzun dönemde takibini de kontrol etmektedir. Ayrıca iç denetçiler, uygun risk yönetimi stratejilerinin geliştirilmesi konusunda; gerektiğinde yönetime danışmanlık hizmeti de vermeli ve yol gösterici bir tutum izlemelidir.

İç Denetçiler Birliği'nin yayınlarında da yer verdiği üzere, risk odaklı iç denetim aşağıdaki adımlardan oluşmaktadır:

- İşletmenin içinde yer aldığı ortamı anlamak
- Ön risk değerlendirmesi yapmak,
- Birkaç yıllık (tercihen en az 3 yıllık) denetim planı yapmak,
- İkinci risk değerlendirmesini tamamlamak,
- İç denetim planını gerçekleştirmek
- Kapanış toplantısını yapmak

- Denetim raporunun iletişiminin doğru yapılması (Thomas 2007:1-6).

İşletmenin içinde yer aldığımı ortamı tanımak derken sadece işletme çevresi değil aynı zamanda işletmenin sürekliliğini sağlamak için kendisine koyduğu hedefler ve bu hedeflere giderken kullanılan iş süreçleri de buraya dahil edilmelidir. Hedefler ve süreçler analiz edilip risk tespitleri yapılmaya başlanmalıdır.

Ön risk değerlendirmesinde işletmedeki risk düzeyini ve operasyonel birimindeki süreçlere yönelik kontrollerin ne kadar uygun olup olmadığı tespit edilmeye çalışılmaktadır. Burada işletmenin ticari profili, örgütsel yapısı, organizasyonel değişiklikler de değerlendirmeye tabi tutulmaktadır. Bu alanlardaki analizler sonucunda, işletmenin süreçlerinin risk haritası çıkarılmış olur.

Ön değerlendirme sonucunda denetim planı hazırlanmaya başlanır. Riskli olarak görülen alanlar oldukça sık (en az yılda bir), daha az riskli konular ise 2-3 yılda bir denetlenecek şekilde planlamalar oluşturulabilir. Hazırlanan denetim planları güncel değişikliklere göre güncellenmelidir.

İkinci risk değerlendirmesinde ise işletmelerde mevcut olan kontrollerin etkilliği denetlenir. İç denetçiler görüşmeler yaparak, gözlemleyerek kontrollerin doğru çalışıp çalışmadığını tespit etmeye çalışırlar. Kontrollerin yeterliliği ve verimliliği de burada gözden geçirilmektedir. İkinci risk değerlendirmesinde belirlenen risklere karşı işletmenin geliştirdiği kontrollerin etkililiği analiz edilir. Bu risk değerlendirmesinde iç denetçi bizzat sürecin içindedir ve kendisi de testleri bizzat yapmaktadır.

Beşinci aşama olan iç denetim planının uygulanması kısmında tüm güncellemeler bitirilip plan nihai hale getirilir ve denetim fiilen başlar. Kararlaştırılan denetim teknikleri kullanılarak denetim icra edilir. Riskli alanlara daha fazla eğilmek, az riskli alanlarda da daha kısıtlı vakit geçirmek doğru olacaktır. (Türedi, Zor, Gürbüz 2015: 15)

Denetim tamamlandıktan sonra işletmenin hem orta hem üst düzey yöneticilerinin katılımıyla mutlaka kapanış toplantısı organize edilmelidir. Bu toplantıda denetim sürecinde yaşanılanlara yönelik olarak denetçiler ve işletmedeki ilgililer arasında kaliteli bilgi paylaşımı yapılması hedeflenmelidir. Bu bilgi paylaşımı önyargılardan uzak şeffaf ve adil bir temel üzerine kurgulanmalıdır. Toplantı sonucunda tarafların fikir birliğine varmaları ulaşılması gereken noktadır.

Kapanış toplantısını müteakip şekilde taslak denetim raporu hazırlanır. Raporda belirlenen tüm riskler düzeyleri (yüksek, orta ve düşük) ile birlikte ifade edilmelidir. Ayrıca bu risklerin ortadan kaldırılması için

yapılabilecekler mutlaka bu taslak raporda yer almalıdır. Risk düzeyi yüksek olarak tespit edilen konularda işletme hemen bir aksiyon almalıdır. Orta olarak belirlenen riskler ile ilgili ise önlem planı oluşturmaya başlamalı, düşük risk düzeyindeki konularda ise çok acil hareket etmesi gerekmese bile o risk ile ilgili kontrollerde değiştirilmesi gereken yerler olduğu açıktır ve bu konuda da işletme detaylı olarak çalışmalıdır. Taslak rapor tamamlandığında denetçiler ve işletme yöneticileri mutabık olmalıdırlar. Mutabakat sonrasında, taslak rapordaki konulara yönelik eylem planları oluşturulmaya başlanır. Nihai denetim raporunda yani denetim raporunun son halinde ise, hem iç denetçinin tespitleri/önerileri hem de yönetimin oluşturduğu eylem planı yer alır. Raporun son hali tüm yöneticiler ile paylaşılmalıdır. Bu aşamadan sonra iç denetçiler, işletmenin rapordaki eylemlerle ilgili aldıkları aksiyonları düzenli olarak takip etmelidir. (Türedi, Zor, Gürbüz 2015: 16)

4.10. İç Denetimin Kurumsal Risk Yönetimindeki Rolü

Günümüzdeki işletmelerde güçlü bir iç denetimin var olması işletmenin kurumsal yönetiminin ve onun devamında kurumsal risk yönetiminin etkili kullanılmasına olanak sağlayan en önemli noktalardan biridir. Burada iç denetçiler kurumsal risk yönetimi uzmanları ile beraber çok ayırıcı ve aynı zamanda destekleyici bir rol oynamaktadırlar. Kontrol değil risk odaklı iç denetim yaklaşımı ile iç denetçiler işletmelerde katma değer yaratılmasına ve yaratılan katma değerin korunmasına ciddi katkıda bulunurlar. Yönetim kuruluna ve tüm işletme yönetimine verdikleri danışmanlık ve güvence hizmeti ile de etkili, güvenilir kurumsal risk yönetimi çıktılarının oluşmasını sağlarlar. Değer yaratma üzerine kurgulanmış yönetim yaklaşımlarının da desteği ile iç denetçiler bu yaklaşımı günden güne daha fazla benimsemektedirler. Neticede yeni yaklaşım yöntemleri ile iç denetim uygulamaları ve kurumsal risk yönetimi süreci iç içe geçen ve birbirinden beslenen uygulamalar olarak karşımıza çıkmaktadır. (Ramamoorti 2003: 14- 15)

Kurumsal risk yönetimi, işletmelerin hedeflerine ulaşabilmesi, stratejilerini gerçekleştirebilmesi yolunda önemli rol oynamaktadır. COSO'nun, 2017 yılında "Strateji ve Performansla Entegre Şekilde-Kurumsal Risk Yönetimi" modeline geçmesi ile işletmenin sahip olması gereken proaktif bakış açısı sayesinde süreç içinde iç denetim birimine de özellikle danışmanlık hizmeti kapsamında önemli görevler düşmektedir. İşletmede KRY sürecinin olmaması durumunda iç denetçiler, danışmanlık hizmeti kapsamında işletmeye koçluk yapabilir, süreç şemalarının çizilmesi, organizasyonel alt yapısının düzenlenmesi, gerekli eğitimlerin verilmesi, yöneticilere kontrol noktasında destek verilmesi gibi konularda yardım ve destekte bulunabilirler. Tüm bu katma değerli çalışmaları gerçekleştirirken dikkat etmeleri gereken nokta, yönetim

adına risk yönetimi sürecine dair icrai faaliyetlerden (risk iştahının belirlenmesi, risk cevaplarının kararlaştırılıp uygulanması gibi) kaçınmalarıdır. (Can, Çetin 2019:153)

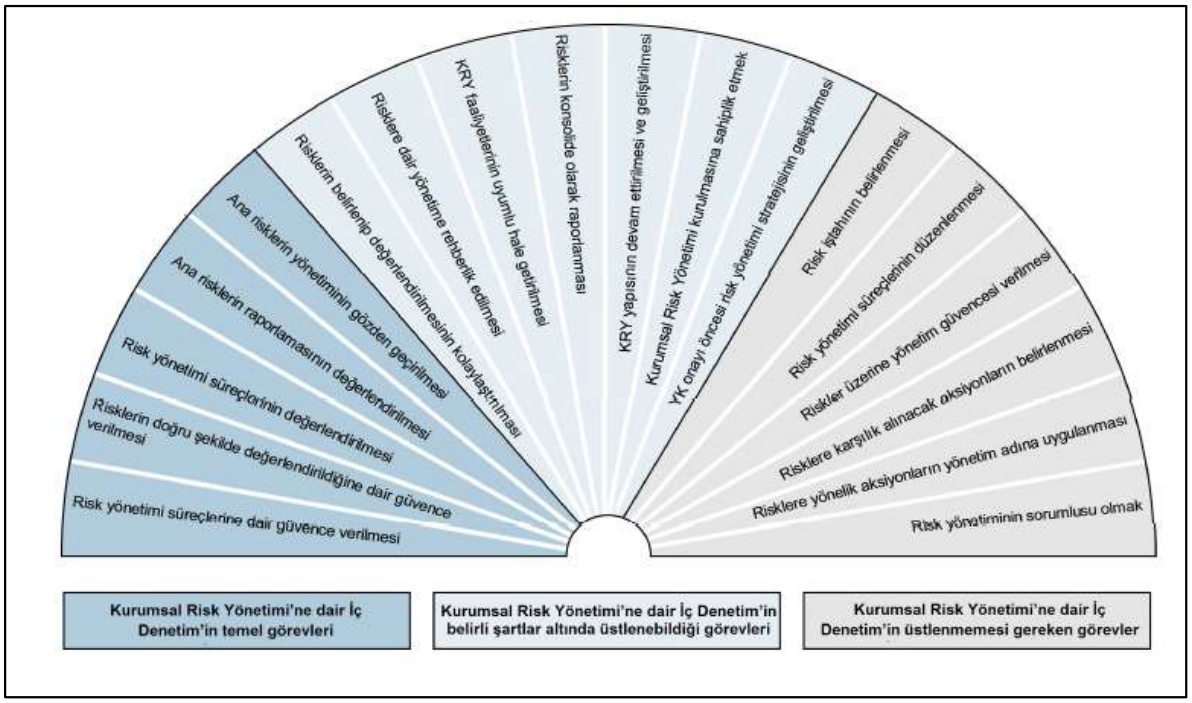
Günümüzde pek çok işletmede ortaya çıkan muhasebe hataları, hilelerinin veya suistimallerinin etkisinin ağır olması nedeniyle üst yöneticiler, kurumsal risk yönetiminin ve iç denetimin bu süreçte etkili uygulanmasına daha çok önem vermekte ve bu konuyla fazlasıyla ilgilenmektedir. Kurumsal risk yönetimi ve iç denetim uygulamalarının takibi; işletmelerin karşılaşabileceği önemli risklerin tespit edilip takip edilebilmesi, etkili şekilde yönetilmesi, raporlanması yönetim kurullarının en önemli görevlerinden biridir. (Mandalas, Can 2020: 79).

Kurumsal risk yönetimi sürecinde, iç denetim faaliyetine çok sayıda sorumluluk düşmektedir. İç denetim, kuruma değer katan güvence ve danışmanlık sağlamaktadır. Bu süreçte iç denetimin ana görevi, iç kontrol sisteminin etkili bir şekilde işlediğini garanti etmek ve işletmenin kurumsal risk yönetimi kapsamındaki faaliyetlerinin yeterli olduğunu göstermektir. Bununla birlikte, bu süreçte iç denetim esnasında yapmak veya yapmamak gereken şeyler vardır. KRY'de iç denetçinin tarafsızlığına ve bağımsızlığına zarar vermemek şartıyla, yönetime yardımcı olurken asla risklerin yönetimini üstlenmeme prensibi temel ilkedir. Aksi yönde hareket etmenin uluslararası normlara da aykırı olacağı açıktır. Öte yandan, dünyada risklerle mücadele konusunda yaşananların, zamanla ülkemizde de yansımaları görülmeye başlamış ve bu hususta ilk olarak finans (bankacılık) sektöründe düzenleyici işlemlerle karşılaşılmıştır. (Bozkurt, 2010: 17-18)

İç denetim; güvence ve danışmanlık hizmetini bağımsız şekilde vermektedir. KRY'ye ilişkin temel rolü ve görevi, risk yönetiminin etkililiği hakkında yönetim kuruluna tarafsız şekilde güvence sağlamaktır. Gerçekten de, araştırmalar, iç denetimin kuruma değer kazandırdığı ve kattığı en önemli iki etkinliğin büyük operasyonel risklerin uygun bir şekilde yönetildiği hakkında güvence sağlamak ve risk yönetimi ve iç kontrol çerçevesinin etkili ve verimli çalıştığı hakkında güvence vermek olduğu konusunda iç denetim birimi ve iç denetçilerin mutabık kaldıklarını göstermiştir.

İç denetim, kurumsal risk yönetimi uygulamalarında önemli rol oynar ve aynı zamanda kurumsal risk yönetimi süreçlerinin varlığı, doğru uygulanıp uygulanmadığı, bu sürecin her aşamasının detaylı tetkiki, risk raporlama çeşitlerinin ve içeriğinin kontrolü, bu süreçteki tüm koordinasyonun denetlenmesi ve tüm bu noktalara yönelik işletmeye güvence verilmesi gibi görevler üstlenmiştir.

Aşağıdaki şekilde görüldüğü üzere, iç denetim organizasyonu bir işletmede kurumsal risk yönetimine dair bazı faaliyetleri kesin üstlenmeli, bazılarında ortak katılımla üstlenmeli ve bazılarını da kesinlikle üzerine almamalıdır. İç denetimin rolünün tespitinde hesaba katılması gereken en önemli faktör, bu faaliyetin iç denetim biriminin bağımsızlığı ve tarafsızlığına yönelik bir tehdit oluşturup oluşturmadığıdır.



Şekil 18: İç Denetimin Kurumsal Risk Yönetimi içindeki Görevlerinin Sınıflandırılması

Kaynak: IIA Pozisyon Raporu: İç Denetimin Kurumsal Risk Yönetiminde Oynadığı Rol, 2009:4

Yukarıdaki şekilde sol tarafta yer alan maddeler, iç denetimin güvence hizmetine yöneliktir ve uluslararası iç denetim standartlarına uygun yapılan bir iç denetimde, iç denetçiler burada belirtilen noktaların en azından bir kısmını yerine getirmelidir. Şeklin ortadaki kısmında yer alan roller iç denetçinin danışmanlık faaliyeti ile ilgili kısımdır. İç denetimde amaç öncelikle güvence faaliyetini yerine getirmek ve sonrasında da danışmanlık faaliyeti ile sürecin iyileştirilmesine katkıda bulunmak olmalıdır. (IIA, 2009, s.5) Şeklin en sağındaki alanda ise, iç denetçilerin üstlenmemesi gereken roller gösterilmiştir. İç denetimin bağımsızlığını ve tarafsızlığını tehdit ettiği düşünülen KRY süreçlerinde iç denetçinin görev almaması gerekir. Bu alandaki roller işletmenin kurumsal risk yönetimi uzmanları/yöneticileri/üst yönetim tarafından gerçekleştirilmesi gereken görevlerdir.

İç denetim, bir işletmenin yönetişim, kurumsal risk yönetimi ve kontrol süreçlerini geliştiren danışmanlık hizmetleri sağlayabilir. Bir iç denetçinin kurumsal risk yönetimine başvurma ölçüsü ve kapsamı, hem yönetim kurulunun erişebileceği diğer iç ve dış kaynaklara hem de kurumun risk olgunluğuna bağlıdır ve bu kapsamın zaman içinde değişmesi de olasıdır. İç denetçinin riskleri değerlendirme ve riskler ile yönetişim arasındaki bağları kavrama ve amaca ulaşmayı yönetebilme konularında uzman olması, iç denetim biriminin özellikle erken aşamalarında kurumsal risk yönetimi için lider olarak ve hatta proje müdürü olarak görev yapmaya ehil ve kalifiye olduğu anlamına gelmektedir. İşletmenin risk olgunluğu arttıkça ve risk yönetimi işletmenin operasyonlarına daha fazla yayıldıkça, iç denetimin kurumsal risk yönetimine liderlik yapma rolü azalabilir. Benzer şekilde, bir kurum bir risk yönetim uzmanının veya fonksiyonunun hizmetlerinden yararlandığı takdirde, iç denetim biriminin daha fazla danışmanlık faaliyetlerine girmektense güvence rolü üzerinde yoğunlaşarak kuruma değer kazandırması olasılığı ve imkanı daha fazladır. (Kara, Sakarya 2012:76)

İç denetimin kurumsal risk yönetimi sürecinde sorumlulukları sırasında dikkat edilmesi gereken noktalar aşağıda yer almaktadır:

- Kurumsal risk yönetimi, işletme yönetiminin sorumluluğundadır.
- İç denetim yönetmeliği, iç denetçinin sorumluluk ve görevlerini açıkça tanımlamalı ve denetim komitesi tarafından onaylanmalıdır.
- İç denetim birimi, işletme yönetimi için herhangi bir riski yönetmemelidir.
- İç denetim birimi, risk yönetimi ile ilgili kararları kendi başına almamalı, işletme yönetiminin karar alma sürecine tavsiye ve önerilerle yardımcı olmalıdır.
- Güvence faaliyetlerinin ötesindeki iş ve görevler, bir danışmanlık görevi olarak algılanmalı ve uygulama standartlarına uyulmalıdır.
- İç denetim, üst yönetime ve yönetim kuruluna, risklerin ve fırsatların doğru bir şekilde yönetilmesini sağlar. Bu, işletmenin iç kontrol sistemlerinin iyi çalıştığını garanti eder.

Uluslararası iç denetim standartlarına göre de risk yönetiminin temel sorumluluğu işletme yönetimine aittir. Bu standartlar, iç denetçilerin yönetimin verdiği kararları yerinde analiz etmelerini, gerekli desteği vermelerini, tavsiyelerde bulunmalarını ancak risk yönetimine yönelik kararları tek başlarına almamaları gerektiğini ifade eder. Aksi takdirde, iç denetçinin tarafsız olma özelliği zedelenmiş olur. Buna ilaveten, iç

denetimin risk yönetimiyle ilgili sorumlulukları denetim komitesi tarafından da onaylanmış olmalıdır. (Kara, Sakarya 2012:77)

İç denetçiler, yönetimin risk yönetimi süreçlerini inceleyerek, değerlendirerek, rapor ederek ve iyileştirmeler önererek yönetime yardımcı olmalıdır. Üst yönetim, işletmenin risk yönetimi ve kontrol prosedürlerinden sorumludur. Bununla birlikte, bu risklerin tanımlanması, değerlendirilmesi, risk yönetimi tekniklerinin uygulanması ve bu risklerle ilgili kontrol önlemlerinin alınması ve uygulanması, iç denetçilerin danışmanlık görevlerini kapsar.
Bir kurumda risk yönetimi sürecinin bulunup bulunmaması, iç denetimin ne kadar önemli olduğunu belirleyecektir. Bazı işletmeler risk yönetimi için yerleşik bir prosedüre sahip olmayabilir. Bu durumlarda, iç denetçi, yönetime bu tür bir sürecin oluşturulmasına ilişkin önerilerini iletmelidir. KRY'nin proaktif hareket tarzının iç denetimin ruhunda da olduğu unutulmamalıdır. İç denetim, riske dayalı olarak çalışır ve bu nedenle, risklerle mücadele sürecinde başarılı olmak için önemli roller oynar. (Bozkurt 2020: 24-25)

İç denetim, kurumsal risk yönetimi ile ilgili tek başına karar almaktan kaçınmalı; yönetimin kararına göre gerekli eleştirilerde bulunmalıdır. Bu noktada iç denetimin, kurumsal risk yönetimi kapsamında tarafsız şekilde güvence vermesi beklenemez. Güvence faaliyetlerinin haricindeki çalışmalar, danışmanlık hizmeti şeklindedir, danışmanlık hizmetine yönelik olarak da iç denetim uygulama standartlarına uyum sağlanmalıdır. Neticede, iç denetim ve kurumsal risk yönetim süreçlerinin ilişkisine baktığımızda her ikisininde işletmelere ciddi oranda katma değer kattığı açıkça ortadadır. Bu kapsamda her çeşit riskin etkili biçimde yönetildiğine dair tarafsız güvence vermek, kurumsal risk yönetimi ile iç kontrol sisteminin etkili biçimde çalışması hakkında danışmanlık sağlamaktır. Öner, Adiloğlu 2019: 69)

İşletmeler, risk yönetiminin yönetime ait bir sorumluluk olduğunu kabul etmelidir. İç denetçiler, risk yönetimi ile ilgili kararları vermekten ziyade, yönetime tavsiyede bulunmalı ve gerektiğinde onları sorgulamalıdır. Yönetim, rapor edilen bulgu ve önerilere yanıt olarak alınması gereken uygun önlemleri seçmekten sorumludur. Bir sorunu "düzeltmeme riski" üst yönetim tarafından her zaman kabul edilebilir. Bu, maliyet veya başka nedenlerle de olabilir. (Bozkurt 2020: 25-26)

İç denetim mekanizması işletmeler içinde değer oluşturmaya çalıştığından, öncelikle risk yönetiminin ilkelerini anlamak ve bunları iç denetim uygulamasına dâhil etmek zorundadır. Bu noktada iç denetçilere tavsiye edilen bazı adımlar aşağıdaki şekilde sıralanabilir: (Can, Çetin 2019: 156).

- İç denetçiler çerçevenin temelini tanımak, anlamak zorundadırlar. İç denetçiler genelde iç kontrollerin yeterliliğine odaklanırlar ve iç kontrol sistemini riskleri azaltabilmek için araç olarak görürler. Ancak COSO 2017'ye göre de iç denetçiler, risk kavramını tanımlamalı, değerlendirmeli, ardından analize tabii tutarak cevaplandırmalı ve en sonunda da cevaplarını gözden geçirirerek raporlamalıdır. Bu silsile olmadan iç kontrolleri etkili biçimde ele almak olası değildir.
- İç denetçiler çoğunlukla iç kontrollerin yeterliliği üzerinde değil aksine riskler üzerinde daha çok durarak üst yönetimin hedef belirlemesi ve bunları gerçekleştirmesi süresince risklerini azaltabilirler. Bu anlayışla hareket eden denetçilerin sayısı arttıkça üst yönetim iç denetimin değer katma işlevini o kadar daha iyi algılayacaktır. Tabii bu noktada iç denetçiler icrai bir tutum içinde olmamalı, neticede yönetimin hedeflerine ulaşmasına destek olmak için çaba harcadıklarının farkında olmalıdırlar.
- İç denetçiler etraflıca düşünmeden sadece riski azaltmaya odaklanmamalıdır. Risk cevapları aynı zamanda, performansı artırmaya yönelik olarak tasarlanmalıdır. Tam bu nokta bize risklerin tehdit olduğu kadar fırsatta olabileceği gerçeğini ifade etmektedir.

Kurumsal risk yönetimi, iç denetime tabi olduğu gibi dış denetime de tabidir. Dış denetimi gerçekleştiren denetçiler, denetimini yaptıkları organizasyon ile ilişkisi olmayan denetçilerdir. Dış denetçilerin kontrol değerlendirmesi yapabilmeleri ve risk yönetiminin kendine has yönleriyle ilgili bilgi ve erişime sahip olmalarından dolayı, organizasyonun kontrol sisteminin değerlendirilmesinde bağımsız izleme faaliyeti kapsamında görev almaktadırlar. Dış denetçilerin, risk yönetim sisteminin yapısını anlaması, kontrol riskinin değerlendirilmesi açısından temel oluşturur. Denetçiler, organizasyonun, kontrol noktalarını gözlemleyerek, belgeleri inceleyerek, yönetim ve çalışanlarla görüşerek kurumsal risk yönetim sistemi hakkında bir izlenime varır ve bağımsız denetim işlevini yerine getirmiş olurlar. Bir işletmede kurumsal risk yönetimi sisteminin düzgün çalışıp çalışmadığının iç denetim dışındaki kontrol mekanizması görüldüğü üzere bağımsız denetimdir. (Akçakanat 2016: 30-46)

5.BIST 50'DE YER ALAN İŞLETMELERDE KURUMSAL RİSK YÖNETİMİ SÜRECİNDE İÇ DENETİMİN ROLÜNÜ VE ETKİLİLİĞİNİ TESPİT ETMEYE YÖNELİK BİR ARAŞTIRMA

5.1. Araştırmanın Kapsamı

İşletmelerin sürdürülebilir büyüme hedefine ulaşabilmeleri, stratejilerini ve amaçlarını gerçekleştirebilmeleri için bünyelerinde genel kabul görmüş çerçeveler temelinde kurumsal risk yönetimi sürecini oluşturmuş olmaları, bu süreç içinde sadece riskleri değil fırsatları da takip etmeleri, KRY sürecini stratejik planlama ve iç kontrol süreçleri ile entegre şekilde yürütmeleri gerekmektedir. İç denetimin üç temel görevinden bir tanesi işletmenin kurumsal risk yönetimi sürecinin etkililiğini değerlendirmektir.

Kurumsal risk yönetimi sürecinin başarısında en önemli unsurlardan bir tanesi kuşkusuz ki etkili bir iç denetimdir. Ancak etkili bir iç denetim mekanizmasının varlığı halinde, o işletmede etkili bir KRY sisteminden bahsedilebilir. Bu noktada kurumsal risk yönetimi olgunluk düzeyi kavramı oldukça dikkat çekicidir.

Araştırma kapsamında BIST-50 işletmelerinde kurumsal risk yönetimi sürecinin gerçekleştirilme adımlarının ve iç denetimin kurumsal risk yönetimi üzerindeki etkililiğinin ortaya çıkarılması, iç denetimin güvence ve danışmanlık hizmeti kapsamında kurumsal risk yönetimi sürecindeki rol ve sorumluluklarını nasıl yerine getirdiğinin ve bu bağlamda kurumsal risk yöneticileri ile iç denetçilerin üst yönetimle olan ilişkilerinin ve işbirliklerinin anlaşılması yer almaktadır.

5.2. Literatür Çalışması

Tez çalışmamız kapsamında yaptığımız literatür taramasında gerek dünyada gerek ülkemizde, KRY ve KRY'nin iç denetimine yönelik çok sayıda çalışma ve araştırma bulunmaktadır. Bu araştırmaların önemli kısmında uygulamaya etkileri bakımından kurumsal risk yönetimi ve iç kontrol ve iç denetim alanındaki standartlar ve çerçeveler incelenmiştir. Bu çalışmaların konumuzla ilgili olanları hakkında aşağıda özlü bilgi verilmiştir.

Kara ve Yereli'nin 2012 yılında hazırladığı "İç Denetimde Risk Yönetimi ve İstanbul Menkul Kıymetler Borsası - İmalat Sanayi Sektöründe Bir Uygulama" isimli çalışmada iç denetim, risk yönetimi, kurumsal risk yönetimi ve risk odaklı iç denetim ile ilgili temel kavramlar anlatılırken, İstanbul Menkul Kıymetler

Borsası-İmalat Sanayi Endeksine kayıtlı şirketlerde risk odaklı iç denetimin, şirketlerin finansal risk düzeyi üzerindeki etkisine ilişkin bir anket çalışmasına ve analize yer verilmiştir. Veri toplama sürecinde kullanılan anket uygulamasına cevap alınan 47 şirket değerlendirmeye alınmıştır. Bunu yanısıra, ankete cevap veren şirketlerin finansal risk düzeylerini belirlemek amacıyla, işletmelerin 2010 yılına ait mali tabloları kullanılarak, seçilmiş likidite, karlılık gibi oranlar ile işletmelerin mali durum analizleri yapılmıştır. Analiz sonucunda, ankete katılan işletmelerde risk yönetim uygulamasının en önemli nedeninin finansal risklerden korunma ve daha etkili bir iç denetim ihtiyacının yer aldığı görülmüştür. İşletmelerin yaklaşık % 40'ı risk yönetim standardı kullanmadıklarını belirtmişlerdir. Ayrıca neticede, iç denetim biriminin risk yönetim sürecinde önemli bir rol aldığı tespit edilmiştir. Yaklaşık %55'lik bir oranla işletmelerin risk yönetim sürecini, iç denetim biriminin kendisinin veya risk yönetim birimi ile beraber gerçekleştirdikleri anlaşılmaktadır. İşletmelerin % 65'i risk odaklı iç denetimin kendi bünyelerinde uygulandığını ifade etmişlerdir.

Gacar tarafından 2017 yılında yapılan "İşletmelerde Kurumsal Risk Yönetimi Kapsaminda Riskin Erken Saptanması ve Yönetimi Komiteleri: Borsa İstanbul'da Nitel Bir Araştırma" isimli çalışmada içerik analizi yöntemi ile 2015 yılında Borsa İstanbul'da yer alan işletmelerin faaliyet raporları aracılığıyla riskin erken teşhisi komitesi ile ilgili analizler yapılmıştır. Çalışma neticesinde, işletmelerin büyük bir çoğunluğunun komite kurulmasına ilişkin yasal zorunluluğa uydukları ancak işletmelerdeki komitelerin kurumsal risk yönetimi sistemi oluşturmada geride kaldıkları tespit edilmiştir.

Onay tarafından 2020 yılından yayınlanan "The Role of Internal Audit from New Enterprise Risk Management Frameworks Perspective: Research in Turkey" adlı çalışmanın temel amacı, KRY faaliyetleriyle ilgili olarak iç denetçilerin faaliyetlerinin zaman içinde ne ölçüde değiştiğini belirlemek ve bu görevlerin pratikte ne ölçüde yerine getirildiğini tespit etmektir. Araştırmada Türkiye'de faaliyet gösteren şirketler t-testi ve varyans analizi (ANOVA) ile analiz edilmiştir. Araştırma sonucunda, bazı iç denetçilerin görüşlerinin demografik değişkenlere (yaş, mesleki tecrübe, sektör tecrübesi) göre farklılaştığı tespit edilmiştir. Sonuçlar benzer çalışmalarla karşılaştırılmıştır. Araştırma sonucunda özel şirketlerdeki iç denetçilerin görev bilincinin kamu sektörüne göre çok daha önde olduğu belirlenmiştir. Yine araştırmaya göre, iç denetçilerin KRY sürecine yönelik bilgi ve birikimlerinin yıllar geçtikçe arttığı gözlemlenmiştir.

Zwaan tarafından 2011'de yayınlanan "Internal Audit Involvement in Enterprise Risk Management" adlı çalışmanın amacı, iç denetçilerin kurumsal risk yönetimine katılımının, risk yönetimi sürecinde rapor

hazırlamaya yönelik istekliliğinin ve bu sürece denetim komitesi ile güçlü bir ilişkisinin olup olmamasının ne derece katkı sağladığının incelenmesidir. Çalışma aynı zamanda Avustralya özel ve kamu sektörü kuruluşlarında KRY süreci ve KRY'de iç denetimin rolünü de araştırmıştır Araştırmada deney tasarımı yöntemi ile 117 sertifikali iç denetçiye ulaşılmıştır. Araştırma sonucunda, iç denetçilerin KRY sürecine katılımı ile risk raporlaması isteği arasındaki doğrudan bağlantı kurulurken, iç denetçilerin denetim komitesiyle olan ilişkisinin bu konuyla bağlantılı olmadığı belirlenmiştir.

Cuevas, Mörtsjö ve Änilane'nin 2015 tarihli "The Process of Internal Audit's Involvement in Enterprise Risk Management: The Influence on Internal Audit's Objectivity and Independence" isimli çalışmasının amacı, iç denetçilerin, kurumsal risk yönetimi faaliyetlerine yoğun katılımının ve üst yönetimle güçlü ilişkilerinin, tarafsızlık ve bağımsızlık üzerindeki etkisini incelemektir. Sonuçta, iç denetçilerin IIA tarafından yayımlanan yönergeleri takip etmenin önemli olduğunu düşündüklerini ve iç denetçiler ile üst yönetim arasındaki güçlü bir ilişkinin, iç denetimin risk sürecindeki aksaklıkları bildirme istekliliğini etkilemediği de görülmüştür.

Drogalas, Eleftheriadis, Pazarskis, Anagnostopoulou tarafından 2014'te yayınlanan "Perceptions about effective risk management. The crucial role of internal audit and management. Evidence from Greece" isimli çalışmanın amacı, etkili risk yönetimi ile ilişkili faktörleri analiz etmektir. Çalışmada veriler, Atina Borsası'nda mevcut şirketlerdeki çalışanlara yapılan anket uygulaması ile toplanmıştır. Etkili risk yönetimi, risk bazlı iç denetim, iç denetçilerin risk yönetimine katılımı ve üst yönetim desteği arasındaki ilişkiyi incelemek için çoklu regresyon analizi yapılmıştır. Sonuçta, risk bazlı iç denetimin, iç denetçilerin risk yönetimine katılımının ve üst yönetim desteğinin etkili risk yönetimi sürecine olumlu katkıda bulunduğu tespit edilmiştir.

Baesley, Clune ve Hermanson'un 2006 yılında yayınladığı "The Impact of Enterprise Risk Management on the Internal Audit Function" adlı çalışmada, keşif araştırması yöntemi ile KRY sürecinin iç denetim faaliyetleri üzerindeki etkisiyle ilgili faktörleri tespit etmek amaçlanmıştır. Araştırma sonunda, KRY sürecinin tamamlanmış olmasının, denetim komitesi ile CFO'nun iç denetime olan yoğun talebinin, baş denetçinin kıdemli olmasının, işletmelerin finansal kuruluş veya eğitim kurumu alanında yer almasının KRY'nin iç denetim üzerindeki etkisini artırdığı gözlemlenmiştir.

Jaber, Shah, Johari ve Mustapha'nın 2024 yılında yayınladığı "The Impact of Internal Audit on Enterprise Risk Management Effectiveness in Jordanian Publiclisted Companies" isimli çalışmanın amacı, Ürdün'deki halka açık şirketlerde iç denetimin kurumsal risk yönetimi süreçlerindeki rolünü ve bu rolün KRY etkililiği üzerindeki etkisini araştırmaktır. Çalışma, çapraz kesitli bir anket yöntemiyle nicel bir metodoloji kullanılarak gerçekleştirilmiştir. Çalışmanın sonucuna göre, iç denetçilerin KRY'deki rolleri orta düzeydedir. Ayrıca, iç denetimin KRY'deki rolü ile iç denetçilerin tarafsızlığının kurumsal risk yönetiminin etkililiği üzerinde olumlu yönde önemli bir katkısı olduğu da görülmektedir.

Günümüzde toplumların ihtiyaç duyduğu işletmeler kurumsal sürüdürülebilir işletmelerdir. Bir işletmenin kurumsal sürüdürülebilirliği o işletmenin dürüst, adil, sorumlu, hesap verebilir ve şeffaflık ilkelerine bağlı ve işletmenin bütün paydaşlarının hak ve menfaatlerini koruyan yönetim anlayışına sahip yöneticilerce yönetilmesidir. Günümüzde bu ilkelere bağlı yöneticilerden işletmenin faaliyetlerinin başarılı olması paydaşlarına sunduğu bilgilerin güvenilir olması ve bütün bunları yasalara uygun şekilde gerçekleştirebilmeleri risk temelli bir iç kontrol sistemi kurmaları ve işletmeleri ve kurdukları bu yapıları bağımsız uzmanlara denetletmeleri beklenmektedir. Hızla gelişen ekonomik ticari ve teknoloji koşullarında işletmeleri tehdit eden risklerin giderek artması ve karmaşık bir hal alması kurumsal risk yönetimini yöneticilerin en büyük sorunu haline getirmiş KRY ve iç denetim gibi erken uyarı sistemlerini ön plana çıkarmıştır Geldiğimiz noktada modern iç denetim iç denetçilere yönetişim denetimi, risk yönetimi denetimi ve kontrollerin denetimi gibi üç önemli görev addetmiştir. Altını çizdiğimiz bu önemine istinaden tez çalışmamızda iç denetimin, kuruluşun risk yönetimi sürecinin denetimini nasıl yapabildiği ülkemizdeki durumu ortaya koyacak şekilde anlaşılmaya çalışılmıştır.

Tezimiz kapsamında yukarıda özetlediğimiz araştırmalardan farklı olarak ülkemizdeki işletmelerde örgütsel konumları itibariyle doğrudan yönetim kuruluna raporlama yapan Kurumsal Risk Yönetimi Birimi ile İç Denetim Birimi arasındaki ilişki araştırılmış ve özellikle iç denetim biriminin, risk yönetim süreçlerinin etkililiğini değerlendirme ve doğrudan yönetim kuruluna raporlama fonksiyonunu etkili bir şekilde yerine getirip getiremediği, risk yönetiminde güvence ve/veya danışmanlık hizmetini ne ölçüde verebildikleri ve görevlerini yaparken bir örgütsel çatışma veya sorun yaşayıp yaşamadıkları ortaya konulmaya çalışılmıştır.

5.3. Araştırmanın Temel Amacı

Yukarıda da açıkladığımız üzere bu araştırmanın temel amacı ülkemizde kurumsal oldukları düşünülen ve KRY ve İç denetim birimlerinin doğrudan Yönetim kuruluna raporlama yaptığı tahmin edilen BİST 50'ye kayıtlı şirketlerde İç Denetim Biriminin güvence ve danışmanlık hizmetleri kapsamında Kurumsal Risk Yönetim Süreçlerini nasıl denetleyebildiklerini ve bu iki örgütsel birimin aralarındaki ilişkiyi ve etkileşimi ortaya koymak kurumsal risk yönetimi seviyelerinin olgunluğu bakımından bir sonuç çıkarabilmektir.

Bu temel amaç doğrultusunda öncelikle söz konusu şirketlerde bu iki birimin standartlara uygun şekilde yapılandırılıp yapılandırılmadığı ve yetkinlik seviyeleri anlaşılmaya çalışılmıştır. Daha sonra KRY sürecinin işleyişi, hangi çerçevelere göre tasarlandığı, KRY sürecinin sorumlularca kontrol, gözetim ve denetiminin nasıl yapıldığı, iç denetçilerin süreci nasıl denetledikleri ve iki birimin arasındaki ilişki ve sorunlar anlaşılmaya çalışılmıştır.

5.4. Araştırmanın Yöntemi

Yukarıda açıklanan temel amaç doğrultusunda önce özellikle COSO ERM ve IIA'in İç Denetim Çerçevelerine uygun bir değerlendirme yapmaya imkan veren sorular hazırlanmış, söz konusu soruların doğrudan BİST 50'ye kayıtlı şirketlerin İç denetim öneticileri/Teftiş kurulu başkanları kıdemli iç denetçileri veya kıdemli KRY uzmanlarına sorulmasına karar verilmiştir. Tez izleme sürecinde hazırlanan sorular BİST 50 ye kayıtlı şireketlerden birinin İç denetim birim başkanı ve kıdemli iç denetçileri ile test edilmiş, ilave görüşler ve düzeltmelerle son şekli verilmiştir.

Araştırma nicel analiz yöntemlerinden birisi olan uygulamalı araştırma şeklinde tasarlanmıştır. Uygulamalı araştırmanın keşifsel, betimsel, ilişkisel olmak üzere farklı türleri bulunmaktadır. Bu araştırma keşifsel bir araştırmadır. Keşifsel araştırmalarda nispeten hakkında az bilgiye sahip olunan konularda küçük ölçekli örneklemlerle konuya ilişkin istatistiklerin sunulması amaçlanmaktadır.

Araştırmanın kapsamında hedeflenen BIST-50 şirketleri, kurumsal risk yönetimi sürecine yönelik mevcut yasal düzenlemeler ve genel kabul görmüş çerçeveler aracılığıyla KRY sistemlerini ve bu süreçlerin gözetimi ve iç denetimini özenle kurgulamak ve uygulamakla yükümlüdürler. Bu nedenle seçilmişlerdir.

BİST 50 Şirketleri faaliyet alanlarına göre dört farklı kategoride yer almaktadır. Bu kategoriler sırasıyla "Bankalar", "Holding", "Üretim" ve "Diğer Hizmetler" şeklindedir. Diğer hizmetler kategorisi yurtiçi / yurtdışı hava taşımacılığı, satış-pazarlama ve lojistik sektöründeki işletmeleri kapsamaktadır.

İşletmelerden örnekleme yöntemiyle veri toplanmıştır. BIST-50'de faaliyet gösteren firmalar bu araştırmanın evrenini oluşturmaktadır. Öncelikle 15 Mayıs 2024 itibariyle bu işletmelerin listesi oluşturulmuş ve işletmelerin yetkilileri ile doğrudan görüşülerek araştırma ile ilgili bilgi verilmiştir. Daha sonra hazırlanan anket formu tüm işletmelere e-mail yoluyla gönderilmiştir. Anket formu gönderilen 50 firmadan 21 tanesinden geri dönüş alınmıştır. Analizler geri dönüş sağlayan 21 firma üzerinden yapılmıştır. Ankete işletmelerin iç denetim biriminde yönetici/ uzman olarak görev yapan çalışanlar cevap vermiştir.

Bu araştırma keşifsel bir araştırma olduğu için, işletmelerin iç denetim süreçlerinde verdiği güvence ve danışmanlık hizmetleri kapsamında kurumsal risk yönetimi sistemin değerlendirilmesine ilişkin durumu ortaya koymaya çalışmaktadır. Bu bağlamda hazırlanan anket formu beş bölümden oluşmaktadır. İlk bölüm görüşülen kişilerin mesleki yeterliliklerinin değerlendirdiği kısımdır. İkinci bölümde kurumsal risk yönetimi ve iç denetimle ilgili genel sorular bulunmaktadır. Üçüncü bölüm iç denetimin kurumsal risk yönetiminin olgunluk düzeyini belirlemesine yönelik sorulardır. Dördüncü ve beşinci bölümdeki sorular ise iç denetimin verdiği hizmetlerin niteliği ile iç denetim sürecinin etkililiğinin ölçülmeye çalışıldığı bölümlerdir.

Çalışmada elde edilen veriler çeşitli istatistiksel yöntemler yardımıyla analiz edilmiştir. Analizler sırasında SPSS kullanılmıştır. Çalışmada verileri analiz yöntemi olarak betimleyici istatistiklerden yararlanılmış, frekans dağılımına ilişkin tablolar ile çapraz tablolar kullanılarak araştırılan konuya açıklık getirilmeye çalışılmıştır.

5.5. Araştırmanın Bulguları ve Yorumlanması

Ankette toplam 47 adet soru yer almaktadır. Anket soruları hazırlanırken uluslararası genel kabul görmüş kurumsal risk yönetimi çerçeveleri ve uluslararası iç denetim standartları ile literatürdeki güncel çalışmalardan faydalanılmıştır.

Anket soruları araştırmacı tarafından oluşturulmuş ve tez izleme sürecinde danışman ve üyelerin katkılarıyla geliştirilmiştir.. Anket soruları hazırlandıktan sonra bir pilot çalışma kurgulanmış, BIST-50

Şirketlerden birinin iç denetim birimi yöneticileri tarafından tüm anket soruları değerlendirilmiş, onların verdikleri geri bildirimlere göre anket revize edilerek son haline getirilmiştir. Yapılan bu çalışma, araştırmanın güvenilirliğine önemli ölçüde katkıda bulunmuştur.

Anket çalışmasına ait sonuç ve bulgulara yer verilirken ilk olarak iç denetim profesyonellerinin ünvanı, sektördeki tecrübeleri ve denetim alanında sahip olduğu belgeler ile çalıştığı firmanın ana faaliyet konusuna ilişkin sektör bilgisi sunulmuştur. Daha sonra firmaların iç denetim birimleri ile kurumsal risk yöntemi süreçlerine ait bilgilere yer verilmiştir. Bu kısımda iç denetim biriminin kurumsal risk yönetimi sürecindeki rolü ve ne derece etkili olduğu çeşitli çapraz sorgulamalar ile ortaya konulmaya çalışılmış, konuya ilişkin örüntülerin varlığı araştırılmıştır. Ayrıca sektör bazında bir farklılık olup olmadığını incelemek için yer yer sonuçlar sektörler açısından da sorgulanmaya tabi tutulmuştur.

5.5.1. Araştırma Kapsamında Yer Alan Şirketlerin ve Katılımcıların Özellikleri ve Değerlendirmeler

Araştırmanın ilk kısmında ankete katılan iç denetim/kurumsal risk yönetimi profesyonellerinin demografik bilgilerine yer verilmiştir. Aşağıda Tablo 15'de katılımcıların ünvanlarına ait dağılım sunulmuştur. Tablo incelendiğinde araştırmaya katılan kişilerin büyük çoğunluğunun (16 kişi) iç denetim yöneticisi veya kıdemli uzman iç denetçi olduğu görülmektedir. Geriye kalan 5 kişinin de kurumsal risk yönetimi süreci ve iç denetimine yönelik bilgi ve tecrübe sahibi oldukları şirketlerle anket öncesi yapılan görüşmelerde teyit edilmiştir.

Tablo 15: Araştırmaya Katılan Kişilerin Ünvanı

Araştırmaya Katılan Kişilerin Ünvanı	**N**
İç Denetim Yöneticisi-Kıdemli Uzmanı	16
İç Kontrolör	2
Kurumsal Risk Yönetimi Yöneticisi-Kıdemli Uzmanı	1
Riskin Erken Teşhisi Komitesi Üyesi	1
İç Kontrol Müdürü	1
Toplam	**21**

Araştırmanın veri toplama aşamasında şirketler ile yapılan görüşmelerde anketi cevaplayacak kişilerin iç denetim/KRY alanında mümkünse 5 yıl ve üzeri tecrübeye sahip olan kişiler olması yönünde talepte bulunulmuştur. İç denetimin önemli bir birikim ve deneyim gerektiren bir meslek olması sebebiyle araştırmanın bu alandaki yetkili kişilerle yürütülmesi hedeflenmiştir . İç denetim alanında yüksek tecrübe sahibi olan kişilerle yapılacak çalışma ile hem daha doğru veri elde edilecek hem de bu durum araştırmayı daha güvenilir kılacaktır. Aşağıda Tablo 16'da araştırmaya katılan kişilerin iç denetim alanındaki tecrübelerine ait bilgiler yer almaktadır. Tablo 16 incelendiğinde katılımcıların büyük kısmının (18 kişi) 5 yıl ve üzeri tecrübeye sahip olduğu görülmektedir.

Buradan anketi dolduran meslek mensuplarının büyük çoğunluğu yeterli deneyime sahip olduğu sonucu ortaya çıkmaktadır.

Tablo 16: Araştırmaya Katılan Kişilerin İç Denetim Alanındaki Tecrübesi

Araştırmaya Katılan Kişilerin Bu İş Alanındaki Toplam Tecrübesi	**N**
0-5 yıl	3
5-10 yıl	5
10 yıl üzeri	13
Toplam	**21**

Araştırmaya katılan kişilerin sahip oldukları sertifikalar, ankette sorulan sorulardan biridir. Bu soru ile, işletmelerin iç denetime verdiği önem ve mevcut iç denetçilerin nitelikleri/yeterlilikleri anlaşılmaya çalışılmıştır.

Aşağıdaki Tablo 17 incelendiğinde 21 katılımcıdan 14 tanesinin iç denetim alanında en az bir sertifikaya sahip olduğu, 7'sinin ise herhangi bir sertifikasının bulunmadığı görülmektedir. Denetim alanında çeşitli sertifikalar bulunmakla birlikte en temel sertifikaların CIA, CRMA, CFE ve SMM-YMM olduğu bilinmektedir. Araştırmaya katılan kişilerin çoğunluğu bu temel sertifikaya sahiptir. Bunun yanında denetim alanında farklı mesleki sertifikalar da bulunmaktadır. Katılımcılar arasında yer alan üretim şirketinde çalışan bir uzman bu sertifikalardan biri olan Scrum proje yönetimine yönelik aşağıdaki tabloda yer alan (SAFe, PSPO 1, PSM, PAL, ICP) 5 adet eğitim sertifikasının bulunduğunu belirtmiştir.

Tablo 17: Araştırmaya Katılan Kişilerin Sahip Olduğu Mesleki Sertifikalar

Araştırmaya Katılan Kişilerin Sahip Olduğu Mesleki Sertifikalar	**N**
Uluslararasi İç Denetçi Sertifikası (CIA)	6
Uluslararası risk yönetimi sertifikası (CRMA)	6
Uluslararası hile denetçisi sertifikası (CFE)	2
SMM-YMM	8
SPKL (SPK Lisansı)	1
SAFe (Çevik Liderlik Eğitimi)	1
PSPO 1 (Profesyonel Scrum Ürün Sahibi Eğitimi)	1
PSM 1(Profesyonel Scrum Master Eğitimi)	1
PAL (Profesyonel Hızlı Liderlik Eğitimi)	1
ICP (Çevik Koçluk Eğitimi)	1
CISA (IT Denetimi)	1
Mevcut Değil	7
Toplam	**21**

Araştırmaya katılan kişilerin çalıştığı işletmelerin faaliyet konusu incelendiğinde Tablo 18'e göre, araştırmanın kapsamı içinde yer alan bütün şirket gruplarından iç denetim profesyonelleri araştırmaya dahil olmuştur. Ayrıca tablodan görüleceği üzere, her sektörden yaklaşık eşit dağılımlı katılımcı araştırmaya katılmıştır. Neredeyse her faaliyet alanından ankete eşit katılım sağlanmış olması araştırmanın güvenilirliğine katkı sunan bir tespittir. Aynı zamanda bu durum, etkili karşılaştırma yapılabilmesini de sağlamıştır.

Tablo 18: İşletmelerin Faaliyet Alanları

İşletmelerin Faaliyet Alanları	**N**
Üretim	5
Finansal Kuruluşlar	6
Holding	5
Diğer Hizmetler	5
Toplam	**21**

5.5.2. Araştırma Kapsamında Yer Alan Şirketlerin Kurumsal Risk Yönetimi Sürecine ve KRY'nin İç Denetimine Verdiği Önemin Analizi

Bu araştırma evreninde yer alan işletmeler borsaya kote işletmelerdir ve bu işletmelerde yönetim kurulu TTK md.366/2 gereğince takdir yetkisini kullanarak iç denetim amacıyla komisyon veya komite kurabilir. Ancak kanun koyucu iç denetimle ilgili iki komitenin kurulmasını zorunlu kılmıştır. Bunlardan ilki, TTK md.375'e göre kurulması gereken denetim komitesidir. Bu komitenin ana görevi, işletmenin denetim sorumluluklarının yerine getirilmesinin sağlanmasıdır. Diğer komite ise riskin erken teşhisi komitesidir. Bu komite ise, denetim komitesine yardımcı bir iç kontrol mekanizması olarak işlev görmektedir. Riskin erken teşhisi komitesi, risklere ve fırsatlara odaklanmaktadır. Denetim komitesinin görevleri arasında ise yönetimin tüm görev ve sorumluluklarının denetlenmesi yer almaktadır.

Kanun koyucu, kurumsal yönetim ilkeleri doğrultusunda md. 378'de ve 625/1-e'de riskin erken teşhisi görevini yönetim kurullarına vermiştir. Bu komitenin kurulması risk yönetimi sürecinin işletmede oluşturulması ve şirketin geleceğinin güvence altına alınması yolunda önemli bir adımdır. İşletmelerde yönetim kurulları bu komite sayesinde risklere zamanında müdahale ederek işletmenin ve tüm paydaşlarının zarara uğramasına engel olacak ve aynı zamanda işletmenin geleceğine yönelik fırsatları da takip ederek yaratılacak katma değere katkıda bulunacaklardır. (Şahin, 206:205)

Bankacılık Kanunu Md.29'a göre; "Bankalar, maruz kaldıkları risklerin izlenmesi, kontrolünün sağlanması, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tâbi ortaklıklarını kapsayan yeterli ve etkili bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlüdürler". Genel hükümlere bakıldığında, bankanın pay senetleri borsada işlem görüyorsa, TTK md.378 gereğince riskin erken teşhisi komitesi kurması gerektiği görülmektedir. Ancak tarih olarak daha sonra yürürlüğe giren Kurmsal Yönetim Tebliği'nde bankalar riskin erken teşhisi komitesinin kurulması konusunda muaf tutmuştur. Ancak risklerin tespiti, ölçümü, izlenmesi ve raporlanması gibi riskin erken teşhisine yarayacak zorunlu görevler vardır. Bu nedenle ilgili komitenin teamülde kurulmuş olmasının işletmeye önemli faydaları vardır. (Şahin, 206:302)

Araştırmaya katılan tüm işletmelerde hem denetim hem de riskine erken teşhisi komitesinin yer aldığı belirlenmiştir. İlgili kanun gereği bu komitelerin yönetim kuruluna belirli aralıklarla raporlama yapması gerekmektedir. Aşağıdaki tablo 19'de görüldüğü üzere, ankete katılan 21 işletmeden 1 tanesi bu soruya

cevap vermemiştir. İşletmelerin büyük çoğunluğu, yani 15 işletmede raporlama sıklığı 4'ten fazla olarak belirtilmiştir. İşletmelerden 4 tanesi 2-4 kez raporlama yaparken, bir işletme yılda bir kez raporlama yaptığını beyan etmiştir. Buradan da görüleceği üzere, TTK Md.378'de de ifade edilen "2 ayda bir raporlama" gerekliliğini sözkonusu birçok işletmenin yerine getirdiği görülmektedir.

Tablo 19 sektörler açısından değerlendirildiğinde ilgili soruya cevap vermeyen işletmenin finansal kuruluşlar sektöründe olduğu, yılda bir kere raporlama yapan işletmenin ise üretim şirketi olduğu görülmektedir. Yine sektörlere göre ortalama en geç 2 ayda bir raporlama yapan işletmeler içinde holdinglerin tamamı yer almaktadır. Ankete katılan 5 holdingin hepsinin aynı raporlama aralığına sahip olduğu görülmektedir.

Tablo 19:Riskin Erken Teşhisi Komitesi'nin 1 Yıl İçinde Yönetim Kurulu'na Sunduğu Rapor Sayısı

	Sektörler				
Riskin Erken Teşhisi Komitesi'nin Yönetim Kurulu'na Sunduğu Rapor Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
2'den az	1	0	0	0	1
2-4 arası	0	1	0	3	4
4'den fazla	4	4	5	2	15
Cevap yok	0	1	0	0	1
Toplam	**5**	**6**	**5**	**5**	**21**

Aşağıda Tablo 20'de riskin erken teşhis komitesinin 1 yıl içinde gerçekleştirdiği toplantı sayılarına yer verilmiştir. Tablodan görüldüğü üzere, ankete katılan 21 işletmeden 1 tanesi bu soruya cevap vermemiştir. Geriye kalan 20 işletmenin 9 tanesi bir yıl içinde 2-4 adet toplantı yaptıklarını beyan ederken yine 9 işletme 4'den fazla toplantı yaptıklarını belirtmiştir. Sadece 2 işletme ise yılda bir toplantı yaptıklarına yönelik cevap vermiştir. Buradan da görüldüğü üzere, net şekilde örneklem içinde yer alan işletmeler sıklıkla yaptıkları toplantılar aracılığıyla işletmenin risk ve fırsat yönetimini takip etmektedirler. Teamüller gereği bu toplantılara katılmadan önce ilgili raporların hazırlanmasıyla da bir hazırlık aşamasından geçtiklerini söyleyebiliriz.

Tablo 20 sektörler açısından değerlendirildiğine, ilgili soruya cevap vermeyen işletmenin bir önceki soruda olduğu gibi finansal kuruluşlar sektöründe olduğu, yılda bir kere toplantı yapan işletmelerin biri üretim diğeri ise "Diğer Hizmetler" alanında faaliyet göstermektedir. Yine sektör kırılımında yılda 2-4 kez raporlama yapan işletmeler içinde holdinglerin ve diğer hizmetler sınıfında yer alan işletmelerin tamamı yer almaktadır. Bir yılda 4'ten fazla raporlama yaptığını söyleyen işletmeler içinde de üretim şirketleri, diğer hizmetler ve 2 adet holding yer almıştır.

Borsaya kote anonim şirketlerin faaliyet raporunda TTK md. 378 gereğince komitenin her iki ayda bir vereceği raporla, şirketin varlığı ve devamını etkileyebilecek risklere yönelik olarak içinde bulunulan dönemi değerlendirmesi, var olan risklere dikkat çekmesi ve bunlara yönelik önlem planları üzerinde görüşmeler yapılması için toplantılar yapıldığı bilinmektedir. Söz konusu işletmeler bu raporlarda hem toplantı sayılarına hem de raporlama sıklıklarına yönelik bilgi vermektedirler. (Töre, 2021: 154) Aşağıdaki tabloda çıkan sonuçlar; ankete cevap veren işletmelerin BIST-50'de yer alması ve kurumsal yönetim ilkelerine uyum derecelerinin yüksek olmasına rağmen, işletmelerin tamamının tavsiye edilen rapor sayısına ulaşamadığını göstermektedir.

Tablo 20:Riskin Erken Teşhisi Komitesi'nin 1 Yıl İçinde Gerçekleştirdiği Toplantı Sayısı

	Sektörler				
Riskin Erken Teşhisi Komitesi'nin Bir Yıl İçinde Gerçekleştirdiği Toplantı Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
2'den az	1	0	0	1	2
2-4 arası	0	4	3	2	9
4'den fazla	4	1	2	2	9
Cevap yok	0	1	0	0	1
Toplam	**5**	**6**	**5**	**5**	**21**

Denetim komitesi, kurumsal yönetim ilkelerine göre, işletmenin iç ve dış denetimin gerekli şekilde yapılmasını sağlayan ve denetim, muhasebe ve mevzuata yönelik deneyime sahip en az iki üyeden oluşmaktadır. (Tüsiad, 2002: 24). Üye sayısı ülkelere, sektörlere, işletmelere göre farklılık gösterebilmektedir. Etkili bir denetim komitesi, kurumsal yönetim ve kurumsal risk yönetimi

mekanizmalarının en gerekli bileşenidir. Yasal düzenlemeler ile özellikle borsaya kayıtlı şirketlerin böyle bir komiteye sahip olmasına yönelik gerekli düzenlemeler yapılmıştır.

İç denetim çalışmalarının neticeleri rapor haline getirilerek iç denetim yöneticisinden denetim komitesine oradan da yönetim kuruluna sunulmaktadır. Bu kapsamda iç denetim faaliyetlerinin denetim komitesi tarafından gözetimi ve izlenmesi olukça kıymetli bir uygulamadır. Bu uygulamanın verimli çalışabilmesi için; denetim komitesi iç denetim planının gerçekleştirilmesinde yer almalı sistemin doğru yapılandırılmasını sağlamalıdır. (Verschoor, 2008;125). Etkili ve sağlıklı çalışan bir iç denetim ortamında denetim komitesi, yönetim ve iç denetim fonksiyonu arasında önceden belirlenen ve düzenli şekilde gerçekleştirilen raporlama terminlerinin ve toplantıların olması çok önemlidir. Hem toplantılar hem de raporlama düzenleri aralarındaki iletişimin durumu hakkında da bilgi sahibi olunmasına yardımcı olmaktadır. (Mollaoğulları, Öncü, 2020: 409) Bu nedenle araştırmada raporlama sıklığı ve toplantı sıklıklarına yönelik sorulara yer verilerek araştırmaya katılan işletmeler için bahsi geçen konuların varlığı incelenmeye çalışılmıştır.

Aşağıdaki Tablo 21'de denetim komitesinin bir yıl içinde Yönetim Kurulu'na sunduğu rapor sayısına yönelik bilgiye yer verilmiştir. Bu bilgiye göre, 21 işletmeden 4 tanesi 2-4 arası raporlama yaptığını, geriye kalan 17 işletmenin ise raporlama sıklığı olarak 4'ten fazla sayıda rapor hazırladığı görülmektedir. Yine tabloya göre, üretim şirketlerinin çoğunluğunun, finansal kuruluşlar ve holding alanındaki işletmelerin de hepsinin 4'ten fazla raporlama yaptığını görmekteyiz. Sonuç olarak, örnek işletmelerde yasal mevzuatlar ve genel kabul görmüş teamüllere uygun şekilde denetim komitesi hazırladığı raporlarını sıklıkla ilgili mercilere sunmaktadır. Bu bulgular neticesinde, üst yönetime gerçekleştirilen raporlama sıklığının çok uzun periyotlarda olmaması denetim bulgularının verimli takip edilebilmesi açısından son derece önemli ve olumludur.

Tablo 21:Denetim Komitesi'nin 1 Yıl İçinde Yönetim Kurulu'na Sunduğu Rapor Sayısı

	Sektörler				
Denetim Komitesi'nin Yönetim Kurulu'na Sunduğu Rapor Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
2'den az	0	0	0	0	0
2-4 arası	1	1	0	2	4
4'den fazla	4	5	5	3	17
Toplam	**5**	**6**	**5**	**5**	**21**

İşletmelerde denetim komitelerinin organize ettiği ve denetim bulgularının, önlem planlarının, önerilerin, yaşanan sıkıntıların nesnel şekilde tartışılabildiği toplantıların sıklığının artırılması iç denetimin etkililiği üzerinde oldukça etkilidir. Aşağıdaki tablo 22'de görüldüğü üzere, ankete katılan 21 işletmenin 14 tanesinde yılda dörtten fazla toplantı yapılırken 7 tanesinde de 2-4 aralığında toplantı yapılmaktadır. Sıklıkları birbirinden farklı olsa da ve TTK, SPK'ya göre yeterli olmasa bile düzenli olarak toplantıların yapılıyor olması ilgili işletmelerde bu konuda bir farkındalığın olduğuna dair izlenim vermektedir.

/

Tablo 22:Denetim Komitesi'nin 1 Yıl İçinde Gerçekleştirdiği Toplantı Sayısının Sektörlere Göre Dağılımı

	Sektörler				
Denetim Komitesi'nin Bir Yıl İçinde Gerçekleştirdiği Toplantı Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
2'den az	0	0	0	0	0
2-4 arası	2	2	2	1	7
4'den fazla	3	4	3	4	14
Toplam	**5**	**6**	**5**	**5**	**21**

Araştırmaya katılan tüm işletmelerde kurumsal risk yönetimi birimleri mevcuttur. Bu birimin işletme içinde bağlı olduğu ve doğrudan raporlama yaptığı birimler Tablo 23'de sunulmuştur. Tabloda görüldüğü üzere, 12 işletmede ilgili birim doğrudan Yönetim Kurulu'na bağlıdır. 6 tanesinde ise öncelikle Riskin Erken Teşhisi Komitesi'ne bağlı çalışmaktadır. Farklı sektörlerdeki kırılımda toplamın kırılımı ile doğru orantılı olmakla birlikte finansal hizmetler alanında genelde Yönetim Kurulu'na bağlı olduğu görülmektedir. Yönetim Kurulu'na bağlı çalışması özerklik anlamında daha rahat çalışmasını da sağlayabilmektedir. Ayrıca doğrudan Yönetim Kurulu'na bağlı birimlerin organizasyon üzerindeki etkisi ve bazen baskısının sürece katkısı olabilmektedir.

Tablo 23: Kurumsal Risk Yönetimi Biriminin Raporlama Yaptığı Bölüm

	Sektörler				
Kurumsal Risk Yönetiminin Raporlama Yaptığı Bölüm	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
Doğrudan Yönetim Kurulu'na bağlıdır.	2	5	2	3	12
Öncelikli olarak Riskin Erken Teşhisi Komitesi'ne bağlıdır.	1	1	2	2	6
Doğrudan Genel Müdür'e bağlıdır.	2	0	0	0	2
CFO'ya bağlıdır.	0	0	1	0	1
Toplam	**5**	**6**	**5**	**5**	**21**

Aşağıda yer alan Tablo 24 kurumsal risk yönetiminde çalışan personel sayısını göstermektedir. Tabloda görüldüğü gibi, işletmelerin yarısından fazlasında bu alandaki çalışan sayısı 0-5 kişi aralığındadır. İçinde üretim şirketleri ve holdinglerin olduğu 6 işletmede ise ekipler 6-15 kişi aralığındadır. Yani bu işletmelerde kurumsal risk yönetimi kadroları diğer işletmelere göre daha geniştir. İşletmelerin büyüklükleri mutlaka burada etkili olan faktörlerden biridir. Ayrıca geniş ekiplerle çalışmak, KRY süreçlerine verilen öneminde bir göstergesi olabilmektedir. Pratikteki örneklerde tüm KRY görevlerinin bir kişiye verilip gerçekleştirilmeye çalışıldığı işletmelerde maalesef ki mevcuttur.

Tablo 24: Kurumsal Risk Yönetiminde Çalışanların Sayısı

	Sektörler				
Kurumsal Risk Yönetimi Bölümünün Çalışan Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
0-5 kişi	2	1	3	5	11
6-15 kişi	3	1	2	0	6
15 kişi üzeri	0	3	0	0	3
Cevap yok	0	1	0	0	1
Toplam	**5**	**6**	**5**	**5**	**21**

Araştırmaya katılan tüm işletmelerde iç denetim birimi mevcuttur. Bu birimin işletme içinde bağlı olduğu ve doğrudan raporlama yaptığı bölümler Tablo 25'de sunulmuştur. Aşağıdaki tabloya göre, 21 işletmenin neredeyse yarısı doğrudan Yönetim Kurulu'na bağlıyken geri kalanı da öncelikli olarak denetim komitesine bağlıdır. Holdinglerde 5 işletmenin 4'ü Yönetim Kurulu'na raporlama yapmaktadır. Bunun tam tersi olarak, üretim işletmelerinde de 4 işletme öncelikli olarak denetim komitesine raporlama yapmaktadır.

Tablo 25: İç Denetim Biriminin Raporlama Yaptığı Bölüm

	Sektörler				
İç Denetim Biriminin Raporlama Yaptığı Bölüm	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
Doğrudan Yönetim Kurulu'na bağlıdır.	1	3	4	2	10
Öncelikli olarak Denetim Komitesi'ne bağlıdır.	4	3	1	3	11
Toplam	**5**	**6**	**5**	**5**	**21**

Aşağıdaki Tablo 26'da iç denetim biriminde çalışan personel sayısına yer verilmiştir. Tabloya göre, iç denetim birimlerinin yarısından fazlasının çalışan sayısı 15 kişi üzeridir. Yani iç denetim birimleri büyük ekipler şeklinde oluşturulmuştur. Ekiplerin kapsamı, işletmede iç denetime verilen önemi gösteren etkenlerden biri olduğu için, bu netice oldukça olumludur. Sadece 2 işletmede toplam kişi sayısı 5'in altındadır. Bu iki işletmede üretim yapan işletmelerdir. İç denetim birimlerinin, işletmelerin büyüklükleri, faaliyet alanları, uluslararası şirket olup olmamaları gibi etkenler göz önüne alınarak belirlenmesi ve tüm bu etkenlerle doğru orantılı olması tavsiye edilmektedir.

Tablo 26: İç Denetim Biriminde Çalışan Sayısı

	Sektörler				
İç Denetim Biriminde Çalışan Sayısı	**Üretim**	**Finansal Kuruluş**	**Holding**	**Diğer Hizmetler**	**Toplam**
0-5 kişi	2	0	0	0	2
6-15 kişi	2	0	2	3	7
15 kişi üzeri	1	6	3	2	12
Toplam	**5**	**6**	**5**	**5**	**21**

İç denetim faaliyetlerinin uluslararası iç denetim standartlarına göre yapılması, iç denetim yönetmeliğinde buna yönelik ibarenin bulunması büyük önem arz etmektedir. İç denetim birimleri, işletmelerin faaliyetlerini geliştirme ve onlara katma değer yaratma görevini yerine getirirken, bir taraftan da kendi faaliyetlerinin etkililiğini gözlemlemelidir. "Kalite Güvence ve Geliştirme Programı"nın oluşturulması ve uygulanması, iç denetim faaliyetlerinin standartlara uygun ve etkili şekilde gerçekleştirildiğinin en büyük güvencesidir. (Akçıl, 2009:108) Bu bakış açısı ile aşağıdaki tablo 27'ye göre, 21 işletmeden 18'i iç denetim birimlerinin uluslararası iç denetim standartlarını referans alarak görevlerini yerine getirdiğini beyan etmişlerdir. Üretim ve diğer hizmetler faaliyet alanında olup uluslararası iç denetim standartlarını referans almayan işletme mevcut değildir. Yine 21 işletmeden 15 işletmede, iç denetim yönetmeliğinde iç denetim çalışma usul ve esaslarını dizenleyen standartlara uygun çalışılacağı ibaresi mevcuttur. 13 işletmede de (6 bankadan birinde) iç denetim birimleri IIA'in uluslarası kalite güvence ve geliştirme programından geçmiştir. Raporlamalarda denetimlerin uluslararası standartlara uygun yapıldığı beyan edilmektedir. Bu tespitlere göre, genel olarak işletmelerin iç denetim faaliyetini standartlar ve çerçevelere göre yapmayı hedeflediği görülmektedir. Ama bazı kapsamlarda gelişmeye açık yönlerinin olduğu da aşikardır.

Tablo 27: İç Denetim Biriminin Uyum Gösterdiği Standartlar/Yönetmelikler

İç Denetim Biriminin Uyum Gösterdiği Standartlar/Yönetmelikler	Üretim (N=5)	Finansal Kuruluş (N=6)	Holding (N=5)	Diğer Hizmetler (N=5)
İç denetim birimi, IIA'in uluslararası kalite güvence geliştirme programından geçmiştir. Raporlamalarda, denetimlerimiz uluslararası iç denetim standartlarına uygun şekilde yapılmıştır ibaresi kullanılmaktadır.	3	5	3	2
İç denetim yönetmeliğinde iç denetim birimi çalışma usul ve esaslarını düzenleyen iç denetim standartlarına uygun çalışılacağı esası yer alır.	4	4	3	4
Uluslararası iç denetim standartlarını referans alarak faaliyetlerini yürütür.	5	5	3	5
Cevap yok	0	0	1	0

İşletmelerde, aşağıdaki tabloda yer alan sertifikalardan en çok CIA ve SMM/YMM ve CFE sertifikalarının var olduğu tespit edilmiştir. İç denetim birimindeki çalışan sayıları ile iç denetçilerin sahip olduğu

sertifikalar birlikte değerlendirilmiş, bu değerlendirmeye göre ortalama belge sayısının 15 kişi üzeri çalışanı olan büyük işletmelerde daha fazla olduğu görülmüştür. Buradan çıkarılabilecek sonuç, büyük ekipler kuran işletmelerin istihdam ettikleri iç denetçilerin sertifika sahipliği oranı yüksektir. Bu da aslında işinin ehli çalışanlarla çalıştıkları şeklinde yorumlanabilmektedir. Aynı şekilde sektör kırılımına bakıldığında sertifika sahipliği holding işletmeleri ve finansal kuruluşlar alanında diğer alanlara göre oldukça fazladır.

Tablo 28: İç Denetçilerin Sahip Olduğu Sertifikalar

İç Denetçilerin Sahip Olduğu Sertifikalar
Uluslararası iç denetçi sertifikası (CIA)
Yeminli mali müşavir (YMM) ya da serbest muhasebeci mali müşavir (SMM)
Uluslararası hile denetçisi sertifikası (CFE)
Uluslararası risk yönetimi sertifikası (CRMA)
Bağımsız denetçi sertifikası (KGK)

5.5.3. Araştırma Kapsamında Yer Alan Şirketlerin Kurumsal Risk Yönetimi Sürecinin İşleyişi ve Bu Sürecin İç Denetiminin Analizi

Kurumsal risk yönetimi, işletmeyi etkileme potansiyeli olan olayları tanımlama, riskleri ve fırsatları yönetmek, işletmenin hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak için oluşturulmuş olan ve stratejilerin belirlenmesinde de kullanılan bir süreçtir. Kurumsal risk yönetimi aslında işletme yönetiminin bakış açısını da yansıtan bir anlayışı ifade etmektedir. İşletmelerin üst düzey yöneticileri, sınırlı kaynaklarını en düzgün şekilde kullanarak işletmenin faaliyetlerinden gelen getiriyi artırmayı sağlama hedefindedirler ve bu esnada karşılacakları tüm riskleri/fırsatları da değerlendirmeleri gerekmektedir. İç denetim işte tüm bu kurumsal risk yönetimi, iç kontrol ve kurumsal yönetim süreçlerinin etkililiğini değerlendirmek ve iyileştirmek amacıyla sistemli ve disiplinli bir yaklaşım ile işletmenin amaçlarına ulaşmasına yardımcı olmaktadır. İç denetimin etkili şekilde yürütülebilmesi için, işletmenin kurumsal risk yönetimi süreçlerinin işletmenin büyüklüğü, sektörü vb etkenlere uygun risk olgunluk düzeyinde gerçekleştirilmesi çok kıymetlidir. Bu bölümde kurumsal risk yönetimi olgunluk düzeyi ve kontrol özdeğerlendirme kavramına yönelik bulgulara yer verilmiştir.

Aşağıda yer alan Tablo 29 işletmelerde uygulanan KRY adımlarını göstermektedir. İşletmelerin tamamında kurumsal risk yönetimi sürecinin yürütüldüğü görülmektedir. Risk belirleme, izleme ve raporlama adımlarının tüm işletmelerde uygulandığını, risk değerlendirme aşamasının bir işletme hariç yine tüm işletmelerde gerçekleştirildiğini görmekteyiz. Tüm işletmelerin risk önceliklendirme yaptığını, 1 işletmenin ise önlem planı yapıp uygulama safhasına risk yönetimi sürecinde yer vermediği tespit edilmiştir. COSO 2017'de yer aldığı haliyle kurumsal risk yönetimi süreci adımlarına işletmelerin titizlikle uyduğu söylenebilmektedir.

Tablo 29: Uygulanan KRY Adımları

	Sektörler				
Uygulanan KRY Adımları	**Üretim (N=5)**	**Finansal Kuruluş (N=6)**	**Holding (N=5)**	**Diğer Hizmetler (N=5)**	**Toplam**
Risk belirleme	5	6	5	5	21
Risk değerlendirme	5	6	5	5	21
Risk önceliklendirme	5	6	5	5	21
Önlem planı yapma ve uygulama	4	6	5	5	20
İzleme	4	6	4	5	19
Raporlama	2	6	5	5	18

İşletmeler kurumsal risk yönetim sistemlerini belirli modelleri temel alarak kendi bünyelerinde oluştururlar. Aşağıda Tablo 30'da araştırmaya katılan işletmelerin hangi modeli esas aldığına yer verilmiştir. Tablo incelendiğinde işletmelerin %86'sında kendi kurumsal risk yönetimi sistemlerini kurarken baz aldıkları modelin COSO kaynaklı olduğunu (Finansal kuruluşlar ve diğer hizmetler alanındaki işletmeler tamamen COSO'ya göre sistemlerini kurmuşlardır.), sadece 1 işletmenin ISO 31000'i temel aldığını ve iki işletmenin de bu soruya cevap vermediğini görmekteyiz. Bu cevaplara göre, COSO'nun zaman zaman ihtiyaçlara binaen revize ederek yayınladığı güncel kurumsal risk yönetimi çerçevesinin pratikte işletmeler nezdinde kabul görmüş olduğunu söylemek mümkündür.

Tablo 30: İşletmede Temel Alınan KRY Modeli

	Sektörler									
İşletmede Temel Alınan KRY Modeli	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
COSO	4	80%	5	83%	4	80%	5	100%	18	86%
ISO 31000	0	0%	0	0%	1	20%	0	0%	1	5%
Cevap yok	1	20%	1	17%	0	0%	0	0%	2	10%
Toplam	**5**		**6**		**5**		**5**		**21**	

Tablo 31'e göre, işletmelerin bir tanesi hariç hepsinde işletmenin kendi oluşturduğu bir kurumsal risk yönetimi yönetmeliği/prosedürü/el kitabı mevcuttur. Böyle bir yönetmeliğe sahip olmayan işletme, diğer hizmetler sektöründedir.

Tablo 31: İşletmeye Özgü KRY Yönetmeliğinin Varlığı

İşletmeye Özgü KRY Yönetmeliğinin Varlığı	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
Evet	5	100%	6	100%	5	100%	4	80%	20	95%
Hayır	0	0%	0	0%	0	0%	1	20%	1	5%
Toplam	**5**		**6**		**5**		**5**		**21**	

Geleneksel risk yönetiminden kurumsal risk yönetimi sürecine geçişte proaktif anlayışın ön plana çıkmasının da etkisiyle her riskin bir fırsat doğuracağı genel olarak kabul görmüş bir görüştür. Bu görüş neticesinde, işletmelerde gerçek erken uyarı sistemi olarak faaliyet göstermesi beklenen risk yönetiminin ancak sadece riskleri değil fırsatları da takip ettiğinde bu amacı gerçekleştirebileceği aşikârdır.

Tablo 32'ye göre, 21 işletmenin 15'inde yani %71'ünde kurumsal risk yönetimi süreci içinde hem riskler hem de fırsatlar takip edilmektedir. Üretim işletmelerinin %60'ı, finansal kuruluşların %50'si, holdinglerin %80'i ve diğer hizmetler alanının tamamı hem riskleri hem de fırsatları takip etmektedir. İşletmelerin 5 tanesinde ise sadece riskler üzerinden sistem çalışmaktadır. Hem riskleri hem de fırsatlarını düzenli takip eden işletmelerin, hedeflerini gerçekleştirme ve sürdürülebilir büyümeye ulaşmada bir adım daha önde oldukları tahmin edilmektedir.

Tablo 32: KRY İçinde Risk ve/veya Fırsat Takibi

	Sektörler									
KRY İçinde Risk ve/veya Fırsat Takibi	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
Riskler ve fırsatlar	3	60%	3	50%	4	80%	5	100%	15	71%
Sadece riskler	2	40%	2	33%	1	20%	0	0%	5	24%
Cevap yok	0	0%	1	17%	0	0%	0	0%	1	5%
Toplam	**5**		**6**		**5**		**5**		**21**	

Stratejilerin daha hedefe dönük oluşturulması, kaynakların verimli kullanımı, stratejik planlama sürecinin ve karar alma süreçlerinin daha sağlıklı verilere dayanabilmesi için bu süreçlerin kurumsal risk yönetimi süreçleri ile bütünleşmiş şekilde ve iç içe yürütülmesi verimliliğin teminatlarından biridir.

Aşağıdaki tablo 33'e göre, işletmelerin 3 tanesi hariç geri kalanında üst yönetimin karar alma mekanizmasının, hedef belirleme çalışmalarının içinde KRY sürecine yer verildiği görülmektedir. Dolayısıyla bu işletmelerde entegre planlama süreçlerinin var olduğu izlenimi oluşmuştur. Ancak bu süreçler birlikte yönetildiğinde işletmeler risklerini/fırsatlarını zamanında fark edip yönetebilmekte ve gerekli aksiyonları alabilmektedirler.

Tablo 33: Üst Yönetimin Karar Alma Mekanizmasında KRY'nin Varlığı

	Sektörler									
Üst Yönetimin Karar Alma Mekanizmasında KRY'nin Varlığı	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
Evet	2	40%	6	100%	5	100%	5	100%	18	86%
Hayır	3	60%	0	0%	0	0%	0	0%	3	14%
Toplam	**5**		**6**		**5**		**5**		**21**	

Risk iştahı kavramı, işletmenin sahip olduğu misyon ve vizyon doğrultusunda kabul edebileceği en fazla risk miktarını tanımlamaktadır. Başka bir deyişle, üst yönetimin herhangi bir önlem planı yapmadan önce alınabileceğine inandıkları risk miktarıdır.(Bozkurt, 2010:19) Risk iştahının belirlenmesi çoğunlukla yüksek olgunluk düzeyindeki işletmelerde görülen bir uygulama adımıdır.

Aşağıdaki tablo 34'te görüldüğü üzere, işletmelerin %86'sı risk iştahı belirlemesi yaptığını, %14'ü ise yapmadığını beyan etmiştir. Seçilen örneklem BIST-50 şirketleri olduğu için, bu şirketlerin hem kurumsal

yönetim hem de kurumsal risk yönetimi düzeylerinin yüksek olduğu bu konuya verdikleri cevaplar ile bir kere daha görülmüştür.

Tablo 34: Risk İştahı Belirleme Adımının Varlığı

	Sektörler									
Risk İştahı Belirleme Adımının Varlığı	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Mevcuttur	3	60%	6	100%	4	80%	5	100%	18	86%
Mevcut Değildir	2	40%	0	0%	1	20%	0	0%	3	14%
Toplam	**5**		**6**		**5**		**5**		**21**	

Aşağıdaki Tablo 35 işletmelerin belirledikleri risk iştahını hangi periyotlarla takip ettiklerini göstermektedir

Tablo incelendiğinde, risk iştahı belirlemesi yapan 18 işletmenin %72'si risk iştahını 6 ay-1 yıllık süreler için belirlediklerini, bu dönem aralıklarıyla gerekli olan durumlarda güncelliklerini beyan etmişlerdir. Holdinglerin tamamı ile finansal kuruluşların %83'ü bu aralıkta takip yaparken üretim şirketlerin bu aralıkta takip yapan bir işletme bile mevcut değildir. İşletmelerin %17'sinde ise bu takip aralığı, 1-2 yıl olarak görülmektedir. Üretim şirketlerinin %67'si de bu aralıkta takip yapmaktadır.

İşletmelerin risk iştahını sık aralıklarla takip etmesi ve risk iştahını güncel tutmaları, sistemin etkili ve verimli çalışmasına önemli katkıda bulunmaktadır. Çünkü işletmenin faaliyeti değiştikçe, iş hacmi arttıkça, rekabet ortamında bileşenler ya da genel ekonomik parametreler değiştikçe mutlaka risk iştahının da güncellenmesi gerekmektedir. Ancak çevresel ve işletmeye özgü olan değişimlere her süreç içinde ayak uydurulursa süreçlerin etkili olması sağlanabilmektedir.

Tablo 35: Risk İştahı Belirleme Aralığı

	Sektörler									
Risk İştahı Belirleme Aralığı	**Üretim (N=3)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=4)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
6 ay-1 yıl	0	0%	5	83%	4	100%	4	80%	13	72%
1-2 yıl	2	67%	0	0%	0	0%	1	20%	3	17%
3 yıl ve üzeri	1	33%	0	0%	0	0%	0	0%	1	6%
Cevap yok	0	0%	1	17%	0	0%	0	0%	1	6%
Toplam	**3**		**6**		**4**		**5**		**18**	

Uluslararası İç Denetçiler Enstitüsü'ne göre, "Kontrol öz değerlendirme, iç kontrolün etkililiğinin incelendiği ve değerlendirildiği bir süreçtir. Amacı gerçekleştirilmek istenen iş hedeflerine makul güvence sağlamaktır." şeklinde tanımlamıştır. Kontrol öz değerlendirme çalışmalarında, çalışanlardan ve yöneticilerden oluşan çalışma grupları eliyle tüm kurumsal risk yönetimi adımları değerlendirmeye tabi tutulmaktadır. Bu süreç iç denetim ve bağımsız denetim sürecinden farklıdır. Özünde kontrol öz değerlendirme, birim yöneticilerinin ve çalışanlarının hedeflerine ulaşabilmek için karşılaşılabilecek riskleri en aza indirmeyi önceleyen bir değerlendirme sürecidir.

Aşağıdaki tablo 36'ya göre, 21 işletmenin %86'sında kontrol öz değerlendirme gerçekleştirilmektedir. Bu oran finansal kuruluşlar ve holdingler için %100 olarak gerçekleşmiştir. Diğer hizmetler alanının %40'ında ve üretim işletmelerinin %20'sinde ise bu yaklaşım uygulanmamaktadır. Kontrol öz değerlendirme yaklaşımını uygullayan işletmelerin, daha çok COSO 2017 ile hayatımıza girmiş olan proaktif kurumsal risk yönetimi anlayışını şirket bünyesine yerleştirmiş olduklarının da bir göstergesidir.

Tablo 36: Kurumsal Risk Yönetimi Biriminin Kontrol Öz Değerlendirme Yaklaşımı

	Sektörler									
Kurumsal Risk Yönetimi Biriminin Kontrol Öz Değerlendirme Yaklaşımı	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Uygulanıyor	4	80%	6	100%	5	100%	3	60%	18	86%
Uygulanmıyor	1	20%	0	0%	0	0%	2	40%	3	14%
Toplam	**5**		**6**		**5**		**5**		**21**	

Tablo 37'de görüldüğü üzere, kontrol öz değerlendirme yöntemini uyguladığını belirten 18 işletme içinde 17 işletme çalışmaları esnasında anket çalışması kullandığını, yine 14 işletme de birebir görüşme ve grup çalışması yöntemlerinden faydalandığını belirtmiştir.

Tablo 37: Kullanılan Kontrol Öz Değerlendirme Yöntemleri

	Sektörler									
Kullanılan Kontrol Öz Değerlendirme Yöntemleri	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Anket çalışması	3	75%	6	100%	5	100%	3	100%	17	94%
Birebir görüşme	2	50%	4	67%	5	100%	3	100%	14	78%
Grup çalışması	2	50%	4	67%	5	100%	3	100%	14	78%

Tablo 38'e göre, kontrol özdeğerlendirme yaklaşımı kullanan 18 işletmeden %39'un bu yaklaşımı finansal risklerin denetimi için %33'ü operasyonel risklerin denetimi için, %22'si ise uygunluk risklerinin denetimi için kullanmaktadır. 18 işletmeden sadece diğer hizmetler alanından bir işletme hepsi şıkkını işaretlemiş ve tüm risk tipleri için bu yaklaşımı kullandığını belirtmiştir.

Tablo 38: İç Denetçilerin KRY Denetiminde Kontrol Öz Değerlendirme Yaklaşımını Kullanma Amaçları

	Sektörler									
İç Denetçilerin KRY Denetiminde Kontrol Öz Değerlendirme Yaklaşımını Kullanma Amaçları	**Üretim (N=4)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=3)**		**Toplam**	**%**
Finansal risklerin denetimi	1	25%	5	83%	1	20%	0	0%	7	39%
Operasyonel risklerin denetimi	1	25%	1	17%	3	60%	1	33%	6	33%
Mevzuat-uygunluk risklerinin denetimi	2	50%	0	0%	1	20%	1	33%	4	22%
Hepsi	0	0%	0	0%	0	0%	1	33%	1	6%
Toplam	**4**		**6**		**5**		**3**		**18**	

Aşağıdaki tabloya göre, işletmelerin büyük çoğunluğu KRY süreçlerinin etkililiğini iç denetim raporlarındaki bulguları önceleyerek takip etmektedir. 21 işletmeden 10 işletme ise, bu takipte çeşitli yazılımlar kullandığını ve risk yönetimi el kitabına göre de değerlendirme yaptığını belirtmiştir. Sadece 8 işletmede kontrol öz değerlendirme çıktılarına bakıldığını belirtmeleri büyük ihtimalle yukarıdaki tablolarda gördüğümüz kontrol öz değerlendirmenin yoğun kullanımı sonucu oluşan değerlendirmelerin iç denetim esnasında kullanıldığı fikrini uyandırmaktadır.

Tablo 39: KRY Sürecinin Etkililiğinin Takip Edildiği Araçlar

	Sektörler									
KRY Sürecinin Etkililiğinin Takip Edildiği Araçlar	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
İç denetim raporlarında yer alan bulgular takip edilir.	3	60%	6	100%	4	80%	5	100%	18	86%
İç denetim-kurumsal risk yönetimi amacıyla kullanılan yazılımlar aracılığıyla takip edilir.	0	0%	3	50%	3	60%	5	100%	11	52%
İşletmede mevcut olan risk yönetimi el kitabı-prosedürüne göre inceleme yapılır.	0	0%	4	67%	4	80%	3	60%	11	52%
Kurumsal risk yönetimi ekibinin kontrol öz değerlendirme kapsamındaki tespitleri dinlenir.	0	0%	3	50%	3	60%	4	80%	10	48%
Cevap yok	0	0%	1	17%	0	0%	0	0%	1	5%

5.5.4. Araştırma Kapsamında Yer Alan Şirketlerin KRY Sürecinin İç Denetiminin Niteliğinin Anlaşılması ve Etkliliğinin Analizi

Uluslararası İç Denetçiler Enstitüsü tarafından yapılan tanımıyla iç denetim; bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacıyla gerçekleştirilen bağımsız, tarafsız bir güvence sağlama ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetimi, kontrol ve kurumsal yönetim süreçlerinin etkili

liğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur. İç denetim risk yönetimi kapsamında, risk yönetimi süreçlerinin

yapısı/yapılanması ve işleyişi, temel riskler olarak sınıflandırılmış olan risklerin yönetilmesi, bu risklerle ilgili kontrollerin ve riskler karşısında alınan diğer tutumların etkililiği, risklerin tam, doğru ve güvenilir şekilde değerlendirilmesi ile risk ve kontrol konu ve durumlarının güvenilir ve uygun şekilde raporlanması konusunda güvence vermektedir. Danışmanlık hizmeti içinde ise, herhangi bir idarî sorumluluk üstlenmeden, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden, niteliği ve kapsamı denetlenen ile birlikte kararlaştırılan istişarî faaliyetler ve bununla bağlantılı diğer hizmetler yer almaktadır. Usul ve yol göstermek, tavsiyede bulunmak, işleri kolaylaştırmak ve eğitim vermek, bu kapsamdaki faaliyet örnekleridir. İç denetçiler, risklere ilişkin koordinasyon, izleme ve raporlamada odak nokta olarak hareket etmek, IIA (İç Denetçiler Enstitüsü) tarafından belirlenen "iç denetim standartlarına" göre iç denetim birimi üstlendiği görevlerde, mesleki bağımsızlığını ve tarafsızlığını korumalıdır. İç denetimin risk yönetimi ile ilgili temel görevi yönetim kuruluna organizasyonun risk yönetimi aktivitelerinin yeterlilik ve etkililiği ile ilgili tarafsız güvence vermektir. Bu sayede iç denetim yönetim kuruluna kurumun risklerinin uygun şekilde yönetildiği ve bu amaçla kurulan iç kontrol sisteminin etkili bir şekilde işletildiği konusunda güvence verir.

Bir kurum, risk yönetimi süreci oluşturmamışsa, iç denetçi, böyle bir sürecin oluşturulmasına ilişkin tavsiyeleriyle birlikte bu konuyu yönetimin dikkatine sunmalıdır. İç denetçi, denetim faaliyetinin risk yönetimi sürecindeki rolü konusunda yönetimin, denetim komitesi ve yönetim kurulunun görüş ve talimatlarını almalıdır. Bir risk yönetim sürecinin geliştirilmesi ve yönetiminde faal rol oynamak "risklerin sorumluluğunu üstlenmek" rolüyle aynı değildir. Risk yönetim süreci bulunmayan kurumlarda iç denetimin rolü "risklerin sorumluluğunu üstlenmek" olmamalıdır. (Akçay, 2011:39-40)

Tablo 40'da görüldüğü üzere, 21 işletmenin %71'inde yıllık denetim planı içinde kurumsal risk yönetimi denetimi mevcuttur. İşletmelerin yıllık denetim planları içinde kurumsal risk yönetimi denetiminin olup olmadığı sektörlere göre incelendiğinde, yıllık planda kurumsal risk yönetimi denetiminin olmadığı sektörler çoğunlukla üretim ve diğer hizmetler alanıdır. Finansal kuruluşlar alanındaki tüm şirketlerde ve holdinglerin %80'inde yıllık planda kurumsal risk yönetimi denetiminin mevcut olduğu görülmektedir.

Tablo 40: İç Denetimin Yıllık Planında Kurumsal Risk Yönetimi Denetiminin Varlığı

	Sektörler									
İç Denetimin Yıllık Planında Kurumsal Risk Yönetimi Denetiminin Varlığı	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
Evet	2	40%	6	100%	4	80%	3	60%	15	71%
Hayır	3	60%	0	0%	1	20%	2	40%	6	29%
Toplam	**5**		**6**		**5**		**5**		**21**	

Yukarıdaki tabloda yer alan sektör dağılımına bakıldığında, yıllık planda kurumsal risk yönetimi denetiminin olmadığı sektörler çoğunlukla üretim ve diğer hizmetler alanıdır. Finansal kuruluşlar alanındaki tüm şirketlerde ve holdinglerin tamamına yakınında yıllık planda kurumsal risk yönetimi denetimi mevcuttur.

Tablo 41'de görüldüğü üzere, 21 işletmeden %76'sı şimdiye kadar kurumsal risk yönetimine yönelik iç denetimden geçmiştir. Bu oran, holdingler ve diğer hizmetler alanında %80 iken finansal kuruluşların tamamı iç denetimden geçmiştir. Şu ana kadar KRY sürecine yönelik iç denetimden geçmeyen şirketlerin çoğunluğu üretim ve diğer hizmetler alanında faaliyet gösteren işletmelerdir.

Tablo 41: Şimdiye Kadar Kurumsal Risk Yönetimi Sürecine Yönelik Bir İç Geçilip Geçilmediğinin Tespiti

	Sektörler									
Şimdiye Kadar Kurumsal Risk Yönetimi Sürecine Yönelik Bir İç Denetimden Geçilip Geçilmediğinin Tespiti	**Üretim**	**%**	**Finansal Kuruluşlar**	**%**	**Holding**	**%**	**Diğer Hizmetler**	**%**	**Toplam**	**%**
Evet	2	40%	6	100%	4	80%	4	80%	16	76%
Hayır	3	60%	0	0%	1	20%	1	20%	5	24%
Toplam	**5**		**6**		**5**		**5**		**21**	

İç denetimden geçen işletmelerin, denetim sürecinde edindikleri tecrübelerin öğrenilebilmesi için aşağıdaki konular incelenmiştir.

Ayrıca, iç denetimden geçen 16 işletmenin 7 tanesinde son 2 yıl içinde kurumsal risk yönetimi politikalarına uygun olmayan uygulamalar tespit edildiğini belirtmişlerdir.

Tablo 42'de yer aldığı üzere, iç denetim tecrübesi olan 16 işletmenin %88'i hem güvence hem de danışmanlık hizmeti alındığı görülmektedir. Yani iç denetçi bu işletmelerde, hem sürecin yürütülmesindeki eksikleri ve problemli alanları belirtmiştir hem de sürece yönelik iyileştirme önerilerinde bulunmuştur.

İki işletmede ise sadece danışmanlık hizmeti alınmıştır. Sadece danışmanlık hizmeti aldığını söyleyen işletmelerin biri finansal kuruluşlar alanında yer almakta diğeri ise holding şirketidir. Diğer soruların cevaplarına verilen yanıtlardan da anlaşıldığı üzere, sözkonusu bu iki şirketin kurumsal risk yönetimi olgunluk düzeyinin yüksek olduğu ve bu nedenle sadece danışmanlık hizmeti aldığı düşünülebilmektedir.

Tablo 42: İç Denetimin KRY'ye Yönelik Verdiği Hizmetler

	Sektörler									
İç Denetimin KRY'ye Yönelik Verdiği Hizmetler	**Üretim (N=2)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=4)**	**%**	**Diğer Hizmetler (N=4)**	**%**	**Toplam**	**%**
Güvence ve Danışmanlık Hizmeti	2	100%	5	83%	3	75%	4	100%	14	88%
Danışmanlık Hizmeti	0	0%	1	17%	1	25%	0	0%	2	13%
Toplam	**2**		**6**		**4**		**4**		**16**	

İç denetim, bağımsız ve tarafsız yürütülmesi gereken bir güvence ve danışmanlık hizmetidir. Kurumsal risk yönetimi sürecinin etkili olabilmesi için, iç denetçinin üstlenmesi gereken, bazı şartlarda üstlenmesi gereken veya kesinlikle üstlenmemesi gereken roller vardır. Bu kapsamda iç denetim, KRY konusundaki temel rollerinin aracılığıyla işletmeye tarafsız güvence sağlamaktadır. İç denetçi, belli şartlarda üstlenebileceği rolleri gerçekleştirirken bağımsızlık ve tarafsızlığının olumsuz etkilenmediğine emin olmalıdır. Aynı zamanda görevini yerine getirirken idari sorumluluk almamaya azami dikkat etmesi gerekmektedir.(Madendere, 2005:6)

Kurumsal risk yönetimi sürecinde iç denetimin üstlendiği rollerin anketi yanıtlayan işletmelerdeki yansımaları aşağıda yer almaktadır. Aşağıdaki 43, 44 ve 45 numaralı tabloları oluşturan sorular, sayfa 132'de şekil 18'de gösterilen kurumsal risk yönetimi iç denetiminde iç denetçinin üstlendiği rollere istinaden hazırlanmıştır.

Tablo 43'de görüldüğü üzere, işletmelerin %75'inden fazlasında risk yönetimine dair güvence verilmesi, risk değerlemesine yönelik güvence verilmesi, aksiyon planına yönelik güvence verilmesi gibi adımlar

gerçekleştirilmektedir. Üretim sektöründe raporlama ve izleme alanında eksik takipler olduğu görülürken diğer hizmetler alanında süreç adımlarının birçoğunda geride kalındığı, uygulanılmadığı görülmektedir. Bu alandaki görevler, iç denetimin mutlaka üzerine alması gereken görevler olduğu için, diğer iki sektöre göre, finansal kuruluşlar ve holding işletmelerinde daha etkili bir iç denetim yapıldığından söz edebiliriz.

Tablo 43: Kurumsal Risk Yönetimi Sürecinde İç Denetimin Üstlenmesi Gereken Görevler

	Sektörler									
Kurumsal Risk Yönetimi Sürecinde İç Denetimin Üstlenmesi Gereken Görevler	**Üretim (N=5)**	**%**	**Finansal Krlş. (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Top.**	**%**
Risk yönetimi sürecine dair güvence verilmesi	5	100%	4	67%	4	80%	4	80%	17	81%
Risklerin doğru şekilde değerlendirildiğine dair güvence vermesi	5	100%	6	100%	3	60%	2	40%	16	76%
Risklere yönelik alınan aksiyonlar alındığına dair güvence vermesi	5	100%	5	83%	4	80%	3	60%	17	81%
Risk yönetimi sürecinin değerlendirilmesi	5	100%	6	100%	4	80%	3	60%	18	86%
Risk raporlamasının ve ana risklerin yönetiminin değerlendirilmesi	3	60%	5	83%	4	80%	2	40%	14	67%
Risklerin tanımlanmasının gözden geçirme	3	60%	5	83%	5	100%	2	40%	15	71%

Tablo 44'de görüldüğü üzere, bazı şartlar oluştuğunda iç denetim birimlerinin üzerine alabileceği roller de içinde holding işletmelerinin tamamında ve finansal kuruluşların %83'ünde KRY sürecinin iyileştirilmesinin üstlenildiği tespit edilmiştir. Diğer sektörlerde de yüzde 60'ında bu rol gerçekleştirilmektedir. İşletmelerin %24'ünde KRY sürecinin ilk kuruluşunda iç denetimin desteğinin alındığı görülmektedir. Tüm bu hizmetler danışmanlık amacıyla gerçekleştirilen hizmetler arasında yerini alır. Özellikle risklere cevap vermede koçluk yapma, strateji geliştirilmesine destek olma gibi konularda işletmelerin tamamının alacakları çok yol olduğu net şekilde görülmektedir. Danışmanlık hizmeti aldıklarını beyan etseler de içerik anlamında danışmanlık hizmetinin birçok adımını almadıkları görülmektedir.

Tablo 44: Kurumsal Risk Yönetimi Sürecinde İç Denetimin Belirli Şartlar Altında Üstlenmesi Gereken Roller

	Sektörler									
İç Denetimin Belirli Şartlar Altında Üstlenebildiği Görevler	**Üretim (N=5)**	**%**	**Finansal Krlş. (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Top.**	**%**
Risklere cevap vermede işletmeye koçluk yapma	1	20%	0	0%	0	0%	2	40%	3	14%
KRY süreci sonunda risklerin konsolide olarak raporlanması	1	20%	1	17%	0	0%	1	20%	3	14%
KRY sürecinin iyileştirilmesi, kolaylaştırılması	3	60%	5	83%	5	100%	3	60%	16	76%
KRY sürecinin işletmede kurulumunun desteklenmesi	1	20%	2	33%	2	40%	0	0%	5	24%
Yönetim kurulu onayı öncesi risk yönetimi stratejisinin geliştirilmesi	1	20%	1	17%	2	40%	1	20%	5	24%

Aşağıda yer alan tablo 45'te, işletmelerde iç denetim biriminin aslında üzerine almaması gereken rolleri görmekteyiz. Bu rollerin genellikle idari görev içerikli olup iç denetimin gerçekleştirmesi halinde yetkisinin dışına taşmasına, bağımsızlığının, tarafsızlığının zedelenmesine sebep olacak görevler olduğu söylenebilmektedir. 21 işletmenin %14'ünde risk iştahı belirlemesi yapıldığı ve yine risk cevapları konusunda karar alma işlevini gerçekleştiren 2 işletme olduğu görülmektedir. İşletmelerin genellikle doğru bir çalışma şekliyle buradan bahsedilen rolleri üstlenmekten kaçındıkları da tespit edilen bir noktadır. Bu rollerin çok dikkatli değerlendirilmesi ve özenle takip edilmesi gerekmektedir.

Tablo 45: Kurumsal Risk Yönetimi Sürecinde İç Denetimin Üstlenmemesi Gereken Görevler

	Sektörler									
İç Denetimin Üstlenmemesi Gereken Görevler	**Üretim (N=5)**	**%**	**Finansal Krlş. (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Top.**	**%**
Risk iştahının belirlenmesi	1	20%	1	17%	0	0%	1	20%	3	14%
Risk yönetimi süreçlerini doğrudan düzenlenip uygulanması	1	20%	0	0%	0	0%	0	0%	1	5%
Risk cevapları konusunda karar alma	1	20%	1	17%	0	0%	0	0%	2	10%
Risk yönetimi için hesap verilebilirliğin sağlanması	1	20%	1	17%	3	60%	3	60%	8	38%

Tablo 46'da ise, KRY iç denetimine yönelik hazırlanan raporun öncelikle kime gönderildiği görülmektedir. 21 işletmenin %52'si öncelikle denetim komitesine, yüzde 5'i (1 işletme) öncelikle riskin erken teşhisi komitesine ve yüzde 38'i ise her iki komiteye birlikte raporlama yaptığını beyan etmiştir. Finansal kuruluşlar alanında büyük çoğunluk öncelikle denetim komitesi derken diğer sektörlerde farklı raporlama tercihleri yer almıştır.

Tablo 46: KRY İç Denetimi Raporunun Sunulduğu Birim

	Sektörler									
KRY İç Denetimi Raporunun Sunulduğu Birim	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Denetim komitesi	3	60%	5	83%	1	20%	2	40%	11	52%
Riskin erken teşhisi komitesi	0	0%	0	0%	1	20%	0	0%	1	5%
Hepsi	2	40%	0	0%	3	60%	3	60%	8	38%
Cevap yok	0	0%	1	17%	0	0%	0	0%	1	5%
Toplam	**5**		**6**		**5**		**5**		**21**	

Tablo 47'ye göre 21 işletmeden sadece yüzde 10'unda (iki işletme) kurumsal risk yönetimi sürecinin iç denetimi esnasında kurumsal risk yöneticileri ile iç denetçiler arasında çatışmalar meydana gelmektedir. Sözkonusu iki işletmede finansal kuruluşlar alanında faaliyet göstermektedir. Bu işletmelerden bir tanesi, ortak akıl ve müzakere yoluyla çatışmaları çözdüklerini bir diğeri ise kendi aralarında genellikle çözülemediğini ve konunun denetim komitesi ile riskin erken teşhisi komitesi arasındaki toplantılarda halledildiğini belirtmiştir.

Tablo 47: KRY İç Denetiminde İç Denetçiler ve Risk Yöneticileri Arasında Çatışmanın Varlığı

	Sektörler									
KRY İç Denetiminde İç Denetçiler ve Risk Yöneticileri Arasında Çatışmanın Varlığı	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Evet	0	0%	2	33%	0	0%	0	0%	2	10%
Hayır	5	100%	4	67%	5	100%	5	100%	19	90%
Toplam	**5**		**6**		**5**		**5**		**21**	

Denetim faaliyetlerinin ise, uluslararası genel kabul görmüş yaklaşıma göre, idarenin dışında fonksiyonel bağımsızlığa sahip bir birim tarafından yürütülmesi gerekmektedir. Bu bağımsızlık, idareden bütünüyle bir bağımsızlık anlamına gelmemektedir. Burada önemli olan denetim biriminin; denetimin planlanmasında, yürütülmesinde, raporlanmasında ve denetim sonuçlarının izlenmesinde herhangi bir baskı ve engellemeyle karşılaşmamasıdır ve bunun garanti altına alınmasıdır. (Akpınar, 2011:288)

Anketi cevaplayan meslek mensuplarının yüzde 86'sı, iç denetim faaliyetlerinde bağımsız ve tarafsız hareket edebildiklerini belirtmişlerdir. Bu durum bize iç denetçilerin görevlerini yaparken üst yönetimden gerekli düzeyde destek aldıklarını da göstermektedir. Oranın bu şekilde yüksek olması iyi olmakla birlikte -iç denetim faaliyetinden en etkili biçimde yararlanabilmek için- bu oranın daha da artması istenen durumdur.

Tablo 48: İç Denetim Biriminin Bağımsız ve Tarafsızlığı

	Sektörler									
İç Denetim Biriminin Bağımsız ve Tarafsızlığı	**Üretim (N=5)**	**%**	**Finansal Kuruluşlar (N=6)**	**%**	**Holding (N=5)**	**%**	**Diğer Hizmetler (N=5)**	**%**	**Toplam**	**%**
Genelde bağımsız olsa bile bazen müdahaleler olmaktadır.	1	20%	1	17%	0	0%	1	20%	3	14%
Tamamen bağımsız ve tarafsızdır.	4	80%	5	83%	5	100%	4	80%	18	86%
Toplam	**5**		**6**		**5**		**5**		**21**	

Aşağıdaki tablo 49'da, iç denetim raporundaki tavsiyelerin işletme için uygulanma oranıyla iç denetim bulgularının işletmede nasıl ele alındığı bilgileri beraber gösterilmiştir. Bu bilgilere göre, 21 işletmeden 18 işletme tavsiyelerin titizlikle gerçekleştiğini ve aynı zaman da da bulguların değerlendirilip her biri için aksiyon alındığını ifade etmiştir. İç denetim sürecinde raporların belli dönemlerde takip edilmesi, mevcut bulguların incelenip değerlendirilmesi ve işletme içinde yapılması gereken değişikliklerin, alınması gereken önlemlerin planlanıp gerçekleştirilmesi sürecin etkililiğinde oldukça önemlidir. Bu nedenle yüksek oranda bu takibin mevcut olması işletmelerin bu konudaki farkındalığının yüksekliğini ve iç denetimin ciddiye alınarak uygulanıp takip edildiğini bize göstermektedir.

Tablo 49: İç Denetim Raporundaki Tavsiyelerin İşletme Tarafından Uygulanma Oranı İle Bulguların Ele Alınış Şekli

	İç Denetim Raporundaki Tavsiyelerin İşletme Tarafından Uygulanma Oranı		
İç Denetim Bulgularının Ele Alınış Şekli	**Evet, titizlikle gerçekleştiriliyor.**	**Kısmen gerçekleştiriliyor.**	**Genel Toplam**
Bulgular belli dönemlerde takip edilir.	1	1	2
Bulgular değerlendirilir ve sadece kritik bulgular ile ilgili aksiyon alınır.	0	1	1
Bulgular ehemmiyetle değerlendirilir ve tüm bulgular ile ilgili aksiyon alınır.	17	1	18
Toplam	**18**	**3**	**21**

Tablo 50'da hem iç denetim biriminin hem de üst yönetimin iç denetim raporundaki bulguları ne sıklıkla takip ettiğini karşılaştırmalı olarak gösterilmiştir. Hem iç denetim birimi hem de üst yönetim açısından bakıldığında 21 işletmenin yarısından fazlasında takip sıklığı 0-3 ay olarak belirlenmiştir. Çoğunluk bu alanda olsa 4-6 aylık veya 7-12 aylık takipler yapan işletmelerde mevcuttur. Sadece bir işletmede ve üst yönetim tarafından takip olmadığı belirtilmiş, bu oldukça dikkat çekici bir sonuçtur. Bu işletmenin faaliyeti alanı ise üretimdir.

Tablo 50: İşletmenin İç Denetim Bulgularını Takip Sıklığı

Dönemler	İç Denetimin Bulgu Takip Sıklığı	Üst Yönetimin Bulgu Takip Sıklığı
0-3 aylık dönemlerde	13	11
4-6 aylık dönemlerde	4	5
7-12 aylık dönemlerde	1	4
Yıllık	3	0
Takip Mevcut Değil	0	1
Toplam	**21**	**21**

Tablo 51'de görüldüğü üzere toplam 21 işletmenin yüzde 81'inde kurumsal risk yönetimi süreci iç denetiminin etkililiğinin değerlendirildiği görülmektedir. Bu konuda bir çalışma yapılmadığını söyleyen dört işletmenin her birinin faaliyet alanı farklıdır. Yani her sektörde, KRY iç denetiminin etkililiğine yönelik çalışma yapmayan işletme bulunmaktadır.

Tablo 51: Kurumsal Risk Yönetimi İç Denetiminin Etkililiğinin Ölçülmesi

	Sektörler									
KRY İç Denetiminin Etkililiğinin Ölçülmesi	Üretim (N=5)	%	Finansal Kuruluşlar (N=6)	%	Holding (N=5)	%	Diğer Hizmetler (N=5)	%	Toplam	%
Evet	4	80%	5	83%	4	80%	4	80%	17	81%
Hayır	1	20%	1	17%	1	20%	1	20%	4	19%
Toplam	**5**		**6**		**5**		**5**		**21**	

Aşağıdaki tabloya göre, yukarıda kurumsal risk yönetimi süreci iç denetiminin etkililiği konusunda çalışma yaptığını söyleyen 17 işletmenin tamamında iç denetim zaman planına uyumunun dikkate alındığı ve yüzde 82'sinde de hem raporun hazırlanma süresi hem de bulguların düzenli takibi konularının bu noktada etkili olduğu belirlenmiştir. Bir holding işletmesi ise bu konuda ISO 9011 KYS kriterlerine uyuma önem verdiğini belirterek konuya farklı bir boyut katmıştır.

Tablo 51: Kurumsal Risk Yönetimi İç Denetiminin Etkililiğini Belirleyen Faktörler

	Sektörler									
KRY İç Denetiminin Etkililiğini Belirleyen Faktörler	**Üretim (N=4)**	**%**	**Finansal Kuruluşlar (N=5)**	**%**	**Holding (N=4)**	**%**	**Diğer Hizmetler (N=4)**	**%**	**Toplam**	**%**
İç denetim planına uygun zamanda iç denetimin tamamlanması	4	80%	5	83%	4	80%	4	80%	17	100%
İç denetim raporunun ne kadar sürede hazırlandığı	3	60%	4	67%	4	80%	3	60%	14	82%
İç denetim bulgularının iç denetçiler tarafından düzenli takip edilip edilmemesi	4	80%	5	83%	3	60%	2	40%	14	82%
ISO 9011 KYS kriterlerine uyum	0	0%	0	0%	1	20%	0	0%	1	6%

6. SONUÇ

Kurumsal risk yönetimi, işletmelerde hem erken uyarı sistemi olarak hem de karar destek sistemlerinin en büyük yardımcısı olarak işlev görmektedir. Kurumsal risk yönetiminin işlevini etkili bir şekilde yerine getirebilmesi için, öncelikle işletmenin her bölümünde/biriminde risk kültürünün mevcut olması ve her seviyedeki çalışanda risk farkındalığının oluşmuş olması gerekmektedir. Risk farkındalığının işletmede yaygınlaştırılması ve risk kültürünün oluşturulmasında kullanılan en önemli araç, işletme içinde KRY süreçlerine yönelik düzenli eğitimlerin verilmesidir. Risk yönetimi, işletmede risklerin/fırsatların belirlenmesi, değerlendirilmesi, izlenmesi ve raporlanması şeklinde adımları olan sistematik bir süreçtir. risk iştahını belirleyen, risk yönetimi süreci adımlarını eksiksiz uygulayan, iç kontrolle ve iç denetim fonksiyonu ile yapıcı iletişim içinde entegre olarak çalışan risk yönetimi sürecine sahip işletmelerde kurumsal risk yönetimi olgunluk düzeyi yüksektir. Bu olgunluğa sahip işletmelerde risk bilgisine dayalı karar alma kabiliyeti yüksek olduğu sebeple kurumsal hedeflere ulaşma ve krizlere daha dayanıklı olma imkanı da daha yüksektir. Bağımsız konumda tarafsız zihniyetle risk yönetim sürecinin etkililiğinin değerlendirmesini yaparak gördüğü önemli yanlışları üst yönetime raporlayan ya da görüş bildiren iç denetim sürecin olgunlaşmasına önemli bir katkı sunmaktadır. Güvence ve danışmanlık hizmetleri kapsamında risk yönetim sürecini izleyen (monitoring yapan) iç denetim aynı zamanda yönetişim ve iç kontrollerin denetimini de başarılı bir şekilde yürütebilmektedir. Burada krtik konu iç denetimin risk yönetim süreci prosedürlerinin tasarlanması ve yürütülmesinde bir sorumluluk üstlenmemesidir. Aksi durumda tarafsızlığı bozulur.

İç denetimin kurumsal risk yönetim sürecinin denetimini yapabilmesi için kendi yetkinlik seviyesinin de yüksek olması gereklidir.

Tez kapsamında BİST 50 şirketleri genelinde KRY sürecinin nasıl tasarlandığı ve uygulandığı ve sürecinin gözetim ve denetimin nasıl yürütüldüğü ve bu konuda iç denetimin nasıl bir rol oynadığı yaptığımız bir araştırmayla anlaşılmaya çalışılmıştır. Ayrıntılı bilgisini önceki bölümde sunduğumuz bu araştırmanın bulgular ışığında Türkiye'nin Borsaya kayıtlı en önemli şirketlerinde altı çizilecek şu sonuçlara ulaşılmıştır:

1) Ankete cevap veren 21 şirketin tümünde tümünde hem denetim komitesi, hem riskin erken teşhisi komitesi hem de KRY birimi ve iç denetim birimi bulunmaktadır. Ancak bu şirketlerden biri yönetim kuruluna ne sıklıkta raporlama yapıldığı sorusuna cevap vermemiş, bir tanesi yılda sadece bir-kez dört tanesi ise yılda 2-4 kez raporlama yaptığını belirtmiştir. 21 Şirketin 15'nin dörten fazla

raporlama yapması olumlu bir sonuçmuş gibi görünse de 5 tanesinin kanuni bir zorunluluk olan iki ayda bir raporlama yapma yükümlülüğünü yerine getirmediğini göstermektedir.

2) Bu şirketlerde riskin erken saptanması komitesinin ne sıklıkta toplantı yaptığına baktığımızda 11 şirketin 2'sinde sadece bir kez kalan 9'unda ise 3- 6 ayda bir toplantı yapıldığı görülmektedir.
3) Yönetim kurulu bünyesinde görev yapan denetim komitelerinin yönetime sunduğu raporlama sıklığına baktığımızda 17 Şirkette 4'den fazla kez raporlama yapıldığı görülürken diğer 4 şirkette yılda 2-4 kez raporlama yapıldığı görülmektedir.
4) KRY biriminin örgütsel konumu incelendiğinde 21 şirketin 12' sinde doğrudan yönetim kuruluna 6' sında riskin erken teşhisi komitesine 2'sinde doğrudan Genel Müdür'e ve 1'inde ise CFO ya bağlı olduğu görülmektedir. KRY doğası gereği işletmenin tüm faaliyetlerini ve çalışanlarını kapsayan bir süreç yönetimidir. Bu özelliği ile iç denetimden ayrılır. Ayrı bir örgütsel birim kurulması iyi bir koordinasyon için gereklidir. Tez çalışmasının yazarı ve danışmanı bu konunun ayrı incelenmesi gerektiği görüşüyle birlikte KRY biriminin doğrudan icra kurulu başkanlığına bağlı olması ve düzenli aralıklarla veya ani raporlama ilişkisiyle yönetim kuruluna, denetim komitesi vb iç denetime raporlama yapması görüşündedir.
5) İç denetim biriminin örgütsel konumu incelendiğinde, İç denetimin 21 şirketin 10'unda doğrudan yönetim kuruluna 11'inde ise öncelikli olarak denetim komitesine bağlı olduğu görülmektedir. İç denetçinin yönetim kurulu ile doğrudan iletişimi ve etkileşimi iç denetim standartlarına göre daha iyi bir uygulamadır.
6) İç denetim birimlerinin büyüklüğünü anlamak amacıyla sorduğumuzda 21 şirketin 12'sinde 15 kişinin üzerinde iç denetçi çalıştırıldığı bunlardan 6'sının finansal kuruluşlarda üçünün ise holdinglerde olduğu anlaşılmaktadır. 7 kuruluş, 6-15 arası bir sayıda iç denetçi ile hizmet vermektedir.
7) KRY biriminde görev yapan personel sayısı incelendiğinde 21 şirketin 11 inde en fazla 5 kişi üçünde ise 15 kişinin üstünde personel çalıştığı anlaşılmaktadır. Söz konusu 3 şirket finans sektöründe faaliyet göstermektedir.
8) İç denetim birimlerinin uluslararası standartlara uygun çalışıp çalışmadığını anlamak amacıyla sorduğumuz sorularda 13 şirketin Kalite güvence denetiminden geçtiği ve raporlamada ''Denetimlerimiz uluslararası iç denetim standartlarına uygun şekilde yapılmıştır'' ibaresini kullanabildiği anlaşılmıştır. Bu 13 şirketin 5 tanesinin finansal kuruluş olduğu görülmektedir. Diğer yandan iç denetim biriminin çalışma usul ve esaslarını düzenleyen iç yönetmeliğinde iç denetimin iç denetim standartlarına uygun yapılacağı ifadesinin yer alıp almadığı sorusuna 15 şirket

olumlu yanıt verirken bu standartları referans alıp almadıkları sorusuna 18 şirket olumlu yanıt vermiştir.

9) KRY adımlarını uygulamadaki becerilerini diğer bir ifadeyle risk olgunluk düzeylerini anlamak amacıyla sorduğumuz altı aşamalı sorularımıza şirketlerin neredeyse tamamı olumlu yanıt vermiş önlem planı yapmada 20 şirket, izlemede 19 şirket ve raporlama 18 şirket olumlu yanıt vermiştir. Bu son üç adımdaki eksiklik söz konusu şirketlerde risk olgunluk düzeyini olumsuz yönde etkileyen bir sonuçtur. Bu sonucun diğer adımları da geçersiz kıldığını söylemek hiç de yanlış olmayacaktır.
10) Şirketlerin uyguladığı niteliği yüksek ve genel kabul gören bir KRY modeli olup olmadığını anlamak amacıyla sorduğumuz soruya 21 şirketin 18'i COSO ERM, 1'i ISO 31000 yanıtını verirken diğer üçünde böyle bir model kullanılmadığı anlaşılmıştır. Bu modellerin denetimi kolaylaştıran yönleri olması sebebiyle önemli olduğunun altını bir kez daha çizmek gerekir. İlk 50' de yer alan şirketlerden sadece üç şirketin bu durumda olması bile ilgi çekicidir.
11) 21 Şirketin biri hariç tamamında bir KRY Yönetmeliği bulunmaktadır. Bu yönetmeliklerin niteliği ve uygulama başarısı ayrı bir inceleme konusu gerektirir. Ancak 50 şirketten birinde bile görülen bu eksiklik önemli olabilir.
12) Risk yönetim sürecinde fırsatların da dikkate alınıp alınmadığını anlamak amacıyla sorduğumuz sorulara 21 şirketin 15'inde hem risk hem de fırsatların izlendiği cevabını verilirken 5' i nde sadece risklere odaklandığı cevabını alınmıştır.
13) Üst yönetimin KRY verilerine dayalı karar alma ve hedef belirleme uygulaması olup olmadığını anlamak amacıyla sorduğumuz sorulara 21 şirketin 18'i olumlu yanıt verirken 3'ü hayır yanıtı vermiştir. Risk iştahı belirleme aşamasının mevcut olup olmadığını anlamak amacıyla sorduğumuz soruya da yine aynı sayıda olumlu ve olumsuz yanıt alınmıştır. Bu üçünün üretim sektöründe faaliyet gösteren BİST 50'ye kayıtlı şirket olması dikkate değer bir bulgudur. Bu 18 şirketin risk iştahı belirleme aralığı da ölçülmüş bunlardan 13 tanesi 6 ay-1 yıl aralığında risk iştahı belirlediklerini söylemişlerdir.
14) KRY birimlerinin kontrol öz değerlendirme yapıp yapmadıklarını anlamak için sorduğumuz soruya 21 şirketin 18 evet cevabı vermiş bu 18 şirketin 17'sinde anket yöntemi diğerlerinde birebir toplantı ve grup çalışması yapıldığı anlaşılmıştır.
15) KRY Sürecinin etkililiğinin nasıl değerlendirildiğini anlamak için sorduğumuz sorulara 21 şirketin 18'inde İç denetim raporlarında yer alan bulguların takip edildiği cevabı alınmıştır.
16) İç denetimin KRY sürecini denetleyip denetlemediğini anlamak amacıyla sorduğumuz ''Yıllık iç denetim planında KRY Denetimine yer verilip verimediği'' sorusuna 21 şirketin 15' i evet 6 sı

hayır cevabı vermiştir. Diğer yandan şimdiye kadar KRY sürecinin bir iç denetimden geçirip geçirilmediğ sorusuna 21 şirketin 16'sı evet, 5'i ise hayır yanıtı vermiştir.

Bu sonuçlara göre denetim planına dahil edilmeyen bir alanın denetlenmeyeceğini söylemek hiç de yanlış olmayacaktır. Nitekim sadece 16 şirketin KRY sürecinin iç denetime tabi tutulduğu bunlardan birinin sadece bir kere denetelendiği anlaşılmaktadır. Bunun nedenini araştırmak ayrı bir inceleme konusu olabilecek niteliktedir.

17) İç denetimin güvence mi danışmanlık hizmetimi verdiğini anlamak için sorduğumuz soruya 16 şirketin 14'ünün hem güvence hem de danışmanlık hizmeti verdiği 2'sinde ise sadece danışmanlık hizmeti verdiği anlaşılmıştır.
18) KRY sürecinde iç denetimin standartlara göre üstlenebileceği görevler sorulduğunda 21 şirketin 17 sinde KRY sürecine ilişkin güvence verildiği, 16 sında risklerin doğru değerlendirildiğine dair güvence verildiği, 17'sinde alınan aksiyonlara yönelik güvence verildiği,18 inde risk yönetimi sürecinin değerlendirilmesi konusunda güvence verildiği, 14'ünde risk raporlaması ve ana risklerin yönetiminin değerlendirilmesinde güvence verildiği, 15 inde ise risk tanımlamasının gözden geçirilmesi konusunda güvence verildiği anlaşılmıştır. Bu sorulara yakın cevaplar alınması 21 şirketin 15-17'sinde risk yönetim süreçlerinin standartlara uygun kapsamda denetiminin yapıldığını söylemek mümkündür.
19) Diğer yandan iç denetimin KRY sürecinde belli şartlarda üstlenebileceği görevlerin neler olduğunu anlamak için sorduğumuz sorulara 21 şirketin 16 'sı KRY sürecinin iyileştirilmesi olarak yanıt vermiştir. Diğer yandan KRY sürecinde iç denetim biriminin üstlenmemesi gereken görevleri üstlenip üstlenmediklerini anlamak amacıyla sorduğumuz sorulara 21 şirketin 1-3'ü üstlendiği cevabı vermiştir. Bu sonuçlar birlikte değerlendirildiğinde aşağı yukarı 16-17 şirkette bilinçli bir KRY denetimi yapıldığını söylemek yanlış olmaz. Ancak 1-3'ünde KRY olgunluk düzeyine gölge düşüren çeşitli sorunlar bulunduğunu söyleyebiliriz.
20) İç denetimin KRY değerlendirme raporunu kimlere sunduğunu anlamak amacıyla sorduğumuz sorulara 21 şirketin 11'i denetim komitesi, 1 tanesi riskin erken saptanması komitesi, 8 tanesi ise hepsi cevabını vermiştir. Bu soru da yönetim kurulu seçeneği yer almadığı sebeple olumsuz bir değerlendirme yapmak doğru olamayacaktır. Zira iç denetim birimleri doğrudan YK na raporlama yapmaktadır. Denetim planına dahil edilen bir denetim alanınına ilişkin görüşler muhtemeldirki iç denetim raporunda yer alabilir.
21) Örgütsel yapıda aynı seviyede konumlandırılmış iki birim olan KRY birimi ve iç denetimi birimi arasında yetki çatışması ve sorunlar olup olmadığını anlamak için sorduğumuz soruya 21 şirketin 19'u hayır, 2'si evet cevabı vermiştir. Diğer yandan bağımsızlık ve tarafsızlığın bundan nasıl

etkilendiğini anlamak amacıyla sorduğumuz soruya ise 21 şirketin 3'ünde bazı müdahalerle karşılaşıldığı 18'inde ise bağımsızlık ve tarafsızlığın korunduğu yanıtı alınmıştır.

22) İç denetimin tavsiyelerinin yönetim tarafından ne ölçüde dikkate alındığını anlamak amacıyla sorduğumuz sorulara 21 şirketin 18'inde dikkate alındığı ve aksiyonların izlendiği cevabı alınırken 3'ünde kısmen cevabı alınmıştır. Esasen bu cevabı sadece 16 şirketin KRY sürecinin iç denetçilerce denetlendiği cevabıyla birlikte değerlendirmek uygun olacaktır.
23) İç denetimin KRY sürecini denetlemedeki başarısının (etkililiğinin) ölçülüp ölçülmediğini anlamak amacıyla sorduğumuz soruya 21 şirketin 17 si evet 4'ü hayır cevabı vermiştir. Bu soru ölçüm faktörleri sorularıyla desteklenmiş olup alınan cevaplarla bu sonuç doğrulanmıştır.

BİST 50 listesinde yer alan şirketler, Türkiye'nin kurumsallaşma anlamında ülkenin en önde gelen şirketleridir. Kağıt üstünde standartlara uygun örgütsel yapılara sahip oldukları görülebilse de uygulamada durumun farklı olabileceğini araştırmalar gösterebilir. Bu şirketlerden bir tanesinin bile batması ülke ekonomisine büyük zararlar verebilecek boyutta olabilir. Bu önemine dayalı olarak yukarıdaki araştırma sonuçları birlikte değerlendirildiğinde anketimize cevap veren 21 şirketten sadece 15 tanesinde standartlara uygun bir KRY sistemi olduğu ve bu sürecin iç denetçilerce usulüne uygun denetlendiğini söylemek mümkündür. Bu sayı 50 önemli şirketin %10'una isabet eder ki, bu oranın daha yüksek olacağı aşikardır ancak BİST 50'ye kayıtlı şirketlerin %10'unda KRY yönetimi bağlamında hala kurumsallaşma sorunlarının olması oldukça dikkate değer bir sonuçtur.

KAYNAKÇA

KİTAPLAR

Adiloğlu, B. (2011*), İç Denetim Süreci ve Kontrol Prosedürleri*, İstanbul: Türkmen Kitapevi.

Alptürk, E. (2008), *Finans, Muhasebe ve Vergi Boyutlarında İç Denetim Rehberi,* Ankara: Maliye ve Hukuk Yayınları.

Arens, A.A. Loebbecke, J.K. (1994), *Auditing An Integrated Approach*, New Jersey: Prentice Hall.

Bakkal, H., Tunç, İ., Kasımoğlu, A. (2016), *İç Kontrol ve Kurumsal Risk Yönetimi*, İstanbul: İdeal Kültür Yayıncılık.

Bakır, M. (2007), *Denetim*, Trabzon: ABP Yayınları.

Derici, O. (2015), *İç Kontrol ve Risk Yönetimi*, Antalya: BEKAD Yayınları, Yayın No:21.

Cömert, N. (2001), *Sermaye Piyasası Aracı Kurumlarında Etkili Bir İç Kontrol Sistemi ve İç Denetim Fonksiyonu*,İstanbul: Lebib Yalkın Matbaası.

Cömert, N. (2019), "İç Kontrollerle İlgili Teorik Çerçeve ve COSO İç Kontrol Yaklaşımı", Kurt, G.,Uçma, T. (Ed.), *Bütünleşik Yaklaşımla KOBİ'lerde Risk Temelli İç Kontrol,* Gazi Kitapevi: 119-198.

Ekici, H. (2015), *Kurumsal Risk Yönetimi*, Konya: Çizgi Kitabevi.

Ergin, H. (2006*), Denetim*, Kütahya: Dumlupınar Üniversitesi Yayınları.

Ergun, T. (2004*), Kamu yönetimi Kuram Siyasa Uygulama*, Ankara: TODAİE Yayınları.

Fikirkoca, M. (2003), *Bütünsel Risk Yönetimi*, Ankara: Pozitif Matbaacılık.

Finke, R.(2005), *Grundlagen des Risikomanagements*, Germany, Wiley-VCH Verlag.

Goetze, U., Henselmann, K. (2001), *Risikomanagement,* Göttingen:Phsica-Verlag.

Gürbüz, H. (1995), *Muhasebe Denetimi*, Eskişehir: Bilim Teknik Yayınevi.

Güredin, E. (2000), *Denetim*, Kırklareli: Beta Yayınları.

Hoffmann, K. (1985), Risk Management – Neue Wege der betrieblichen Risikopolitik, Karlsruhe: K.Elser GmbH.

Kardeş, S., Özbek, C. (2018), *İç Denetim*, Ankara: Nobel Kitap.

Kıral, H. (Ed.) (2014), *İç Denetim "Yönetime Değer Katmak",* Ankara: İç Denetim Koordinasyon Kurulu Yayınları.

Kıral, H. (Ed.), (2014), *Bilgi Teknolojileri Denetimi: Gelişimi, Temel Kavramlar ve Denetim Alanları, İç Denetim " Yönetime Değer Katmak",* Ankara: İç Denetim Koordinasyon Kurulu Yayınları.

Maliye ve Hesap Uzmanları Derneği (1999), *Denetim İlke ve Esasları*, İstanbul.

Kurt, F.Reding and Others,(2007), *Internal Auditing Assurance & Consulting Services*, The IIA Research Foundation.

Marchetti, A., (2012), *Enterprise Risk Management Best Practices*, New Jersey: John Wiley & Sons.

Ohler, A., Unser, M. (2002), *Finanzwirtchaftliches Risikomanagement*, Germany, Springer Verlag.

Olson, D. L., Desheng W. (2015), *Enterprise Risk Management in Finance*, New York: Palgrave Macmillan.

Özbek, C.Y. (2018), *İç Denetim*, Ankara: Nobel Yayınları.

Özbek, Ç. (2012), *İç Denetim Kurumsal Yönetim, Risk Yönetimi, İç Kontrol*, İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.Cilt No:1.

Özbek, Ç. (2012), *İç Denetim Kurmsal Yönetim, Risk Yönetimi, İç Kontrol*, İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.Cilt No:2.

Özgül, B., Tarhan Mengi, B. (2016), *Kurumsal Sürdürülebilirlik ve Güvencesi"İç Denetim*", İstanbul: Beta Yayınları.

Pehlivanlı, D. (2014), *Modern İç Denetim*, İstanbul: Beta Yayınları.

Pickett, K.H.Spencer , (2005), *Auditing the Risk Management Process", The Ultimate Risk Management Tool*, England: John Wiley&Sons.

Pickett, K.H.Spencer and Pickett, J., (2005), *Auditing for Managers, The Ultimate Risk Management Tool*, England: John Wiley&Sons.

Pickett, K.H.Spencer (2003), *T,he Internal Auditing Handbook*, England: Wiley&Sons Ltd.

Sakin, T. (2017), *İç Kontrol Sistemi ve İç Denetim*, İstanbul: Çağlayan Yayınevi.

Sobel, P.(2005), *Auditors Risk Management Guide Integrating Auditing and ERM*, USA: CCH Incorporated.

Schöning, S., Göğüş, H., Persteiner, H. (2018), *İşletmelerde Risk Yönetimi*, İstanbul, İstanbul Bilgi Üniversitesi Yayınları.

Verschoor, C. C. (2008), *Audit Committee Essentials*, New Jersey: John Wiley & Sons.

Weygant, J. K, Kimmel, P. (2002), *Accounting Principles*, New Jersey: John&Wiley Sons Ltd.

Yılancı, Münevver (2006*), Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma,* Ankara: Nobel Yayınları.

TEZLER

Akkaya, G. (2011), Risk Odaklı İç Denetim ve Risk Odaklı İç Denetim Planlamasında Risk Matrisinin Oluşturulmasına Yönelik Örnek Bir Uygulama, Yüksek lisans tezi, Zonguldak, Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Enstitüsü.

Azaltun, M.(1998), Otel İşletmelerinde Hata Ve Hile Önleme Aracı Olarak İç Kontrol, Doktora Tezi, Eskişehir, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Görener, Ö. (2010), Risk Odaklı İç Denetim: Olasılık-Etki Analizi Çerçevesinde Bir Uygulama, Yüksek Lisans Tezi, İstanbul, Yıldız Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Yılmaz, A.(2007), Havaalanlarında Kurumsal Risk Yönetimi Atatürk Havalimanı Terminalleri İşletmesi için Kurumsal Risk Yönetimi Model Önerisi, Doktora Tezi, Eskişehir, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

MAKALELER

Akçakanat, Ö. (2016),"Kurumsal Risk Yönetimi ve Kurumsal Risk Yönetim Süreci", *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 4/7: 30-46.

Akçay, G. (2011),"Kurumsal Risk Yönetiminde İç Denetimin Rolü ve Kamu İdarelerinde Yaşanan Gelişmeler", *Denetişim Dergisi*, 7: 108-113.

Akçıl, M. (2009)," İç Denetimde Kalite Güvence Ve Geliştirme Programı ", *Denetişim Dergis*i, 2: 25-46.

Akpınar, M. (2011),"Denetim Anlayışı ve Metodolojisinde Değişimin Adı: İç Denetim", *ZKÜ Sosyal Bilimler Dergisi*, 7/14: 285-305.

Allan, N., & Davis, J. (2006), "Strategic Risks Thinking About Them Differently", *Proceedings of the Institution of Civil Engineers-Civil Engineering*, 159/6: 10-14.

Anderson, J. Doug, (2017), "COSO ERM Getting Risk Management Right" *Internal Auditor*, 74/5:38-43.

Baloğlu, G., Ülker, M., Adiloğlu, (2019),"İşletmelerde İç Denetimin Rolü: Türk Finans Sektöründe Bir Araştırma", *Muhasebe Enstitüsü Dergisi*, 16/59: 37-46.

Beasley, M. S., Clune, R., Hermanson, D. R, (2005), " Enterprise Risk Management: An Empirical Analysis Of Factors Associated With The Extent Of İmplementation", *Journal of Accounting and Public Policy*, 24/6: 521-531.

Beasley, M. S., Branson B.C., Hancock B.V., (2008), "Rising Expectations, Journal of Accountancy", *ABI/INFORM Global*, 205: 44-51.

Bozkurt, C. (2010), "Risk, Kurumsal Risk Yönetimi ve İç Denetim", *Denetişim Dergisi*, 4: 17-30.

Burnaby, P. ve S. Hass (2009),"Ten Steps to Enterprise-Wide Risk Management", *Corporate Governance*, *The international journal of business in society*, 9/5: 539-550.

Can, E.N. Çetin, C. (2019), "COSO ERM 2017 Çerçevesinde Yönetiminde İç Denetimin Rolü", *Sosyal Bilgiler Dergisi*, 41:153-166.

Cordell, D.M. (2002), "Risk Tolerance in Two Dimensions", *Journal of Financial Planning*,15/5:30-35.

Coşkun, Y. (2009),"Etkili Risk Yönetiminde Öz Disiplin Süreci", *Journal Of Accounting And Taxation Studies*, 2/2: 33-52.

Cox, Louis Anthony (Tony) (2008), "What's Wrong with Risk Matrices? Risk Analysis, *An International Journal,* 28/2: 497-512.

Cömert, N. (2008), "Türk Ticaret Kanunu Kapsamında İç Denetim ve Kontrol", *TİDE İç Denetim Dergisi*, 21:24-27.

Cömert, N. (2016), "İşletmelerde Kontrol ve Denetim Kavramlarının Doğru Kullanılması Amacına Yönelik Kavramsal Bir İnceleme", Marmara Üniversitesi Business Review, 1/1:1-20.

Çakınberk, A. (2010),"Stratejik İttifaklarda Risk Faktörleri Ve Risk Yönetimi", *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 20/1:354-367.

Çeliktaş, B. (2018),"Risk Değerlendirme Karar Matrisi Yöntemi Kullanarak Örnek Bir Risk Değerlendirme Raporunun Oluşturulması", *The Journal of Academic Social Science Studies*, 1/65: 483-504. http://dx.doi.org/10.9761/JASSS7527

Demir Pali, Ç., Adiloğlu, B. (2020),"Kontrol Edilebilen Riskler Ve Risk Yönetimi Açıklamaları: Borsa İstanbul Uygulaması" *Mali Çözüm Dergisi,* 30/157: 77-102.

Emhan, A. (2010), "Risk Yönetim Süreci ve Risk Yönetmekte Kullanılan Teknikler", *Atatürk Üniversitesi İktisadi Ve İdari Bilimler Dergisi*, 23/3: 209-220.

Ermisket, E. G. (2016),"Kamu Kurumlarında Risk Yönetimi-Bir Uygulama Önerisi", *Denetişim Dergisi*, 7: 47-60.

Frigo, M. L., & Anderson, R. J. (2011), "Strategic Risk Management: A Foundation For Improving Enterprise Risk Management and Governance", *The Journal of Corporate Accounting & Finance*, 22/3:81-88.

Florea, R., Florea (2016), "Internal Audit and Risk Management. ISO 31000 and ERM Approaches" *Economy Transdisciplinarity Cognition* 19/ 1: 72-77.

Gacar, A. (2017),"İşletmelerde Kurumsal Risk Yönetimi Kapsaminda Riskin Erken Saptanması Ve Yönetimi Komiteleri: Borsa İstanbul'da Nitel Bir Araştırma", *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, 52: 123-133.

Glowka, G., Kallmünzer, A., Zehrer, A. (2021), "Enterprise Risk Management in Small and Medium Family Enterprises: The Role of Family Involvement and CEO Tenure", International Entrepreneurship and Management Journal, 17/3: 1213-1231.

Güler, A. & Arkın, A. K. (2018),"COSO 2017 Kurumsal Risk Yönetimi Çerçevesine Kontrol Öz Değerlendirme Yaklaşımıyla Bakış Ve Bir Kurum Uygulaması-I" Denetişim Dergisi, 18: 45-62.

Güler, A. & Arkın, A. K. (2019), "COSO 2017 Kurumsal Risk Yönetimi Çerçevesine Kontrol Öz Değerlendirme Yaklaşımıyla Bakış ve Bir Kurum Uygulaması-II". Denetişim Dergisi, 19: 89-100.

Ilgar, T. Erdoğdu, G. (2018),"Kurumsal Risk Yönetimi Türk Kamu Yönetimine Nasıl Entegre Edilebilir?", Denetişim Dergisi, 18: 63-76.

Kara, S.,Sakarya Ş. (2012), "Kurumsal Risk Yönetimi Çerçevesinde Risk Odaklı İç Denetim ve İMKB Uygulaması", Muhasebe ve Vergi Uygulamaları Dergisi, 5/1:69-95.

Kara, S.,Yereli, A. N. (2012),“İç Denetimde Risk Yönetimi Ve İstanbul Menkul Kıymetler Borsası - İmalat Sanayi Sektöründe Bir Uygulama“, Muhasebe Ve Finansman Dergisi, 54: 65-86.

Karaca, S., Şenol, Z. & Korkmaz, Ö. (2018),“Kurumsal Yönetim ile Kurumsal Risk Yönetimi Arasındaki İlişki: Borsa İstanbul Örneği“, Muhasebe ve Finansman Dergisi, 78: 235-248. https://doi.org/10.25095/mufad.412709

Karcıoğlu, R., Kurnaz, E. & Güner, M. (2019), “Bist Kurumsal Yönetim Endeksi Kapsamındaki Şirketlerin Kurumsal Risk Yönetimi Farkındalığı Üzerine Bir Araştırma“, Muhasebe ve Denetime Bakış, 19/58: 103-118.

Karaman, H. C. & Tosuner, M. (2020),“Stratejik Planlama, İç Kontrol ve Kalite Yönetiminde Risk Yönetimi Süreçleri“, Denetişim Dergisi, 21: 98-113.

Keskin, D. A. (2016), “İşletmelerin Sürekliliğini Sağlamada Kritik Öneme Sahip Risk Yönetimi Ve Risk Odaklı Denetim Yaklaşımı, Denetişim Dergisi, 4: 38-46.

Kıral, H. (2018),“Kurumsal Risk Yönetiminin Riskleri”, Denetişim Dergisi, 18: 5-14.

Kızılboğa, R. (2013),“Geleneksel Risk Yönetiminden Kurumsal Risk Yönetim Sistemine Geçiş“, Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 16/3: 297-316.

Kızılboğa, R. (2013), “Kurumsal Risk Yönetimi Odaklı İç Denetim İstanbul Büyükşehir Belediyesi için Bir Model Önerisi”, Marmara Belediyeler Birliği, 24:365-391.

Kishali, Y. & Pehlivanli, D. (2006),“Risk Odaklı İç Denetim ve İMKB Uygulaması“, Muhasebe ve Finansman Dergisi, 30: 75-87.

Koban, A. O., & Karakaya, G. (2022),“Enron Vakası’nın Denetim, Risk Yönetimi ve İç Kontrol İlkeleri Çerçevesinde İncelenmesi“, Denetişim Dergisi, 24: 91-106.

Korkmaz, G. (2020),“İç Kontrol, Risk Yönetimi ve Kurumsal Yönetim Süreçlerinin Değerlendirilmesine Yönelik Ölçeklerin Güvenilirlik ve Geçerlilik Çalışması“, Dokuz Eylül Üniversitesi İşletme Fakültesi Dergisi, 21/1: 177-201. https://doi.org/10.24889/ifede.669663

Köroğlu, Ç. Uçma, T. (2006). “İşletmelerdeki İç Kontrol Sisteminin Etkililiği ve Dış Denetimdeki Önemi”, Mevzuat Dergisi, 103: 2-7.

Küçüközmen, C., (2012),“Yeni Türk Ticaret Kanunu Ve Risk Yönetimi“, Ekonomik Çözüm Gazetesi, 66.

Kurt, G., Uysal, T. (2018),” COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler ”, Muhasebe ve Denetime Bakış Dergisi, 18/54: 19-34.

Lienberg, A.P ve Hoyt, R.E (2003), “The Determinants of Enterprise Risk Management. Evidence From The Appointment of Chief Risk Officers”, Risk Management and Insurance Review. 6/1: 37-52.

Lindow, P. E., & Race, J. D. (2002), ‘’Beyond Traditional Audit Techniques’’, Journal of Accountancy, 194/1: 28-29.

Lo, R.(2016), “The Role of Internal Auditors in Enterprise Risk Management, Risk Management, 7: 46-47.

Mandalas, M., & Can, E. N. (2020), “Kurumsal Risk Yönetimi Kapsamında Risk Odaklı İç Denetim Analizi; Marmara Bölgesindeki Devlet Üniversitelerine Yönelik Bir Araştırma”, Denetişim Dergisi, 20: 78-95.

Mengeş, E., & Aygün, M. (2023),“Kurumsal Risk Yönetimi ve Firma Performansı: Borsa İstanbul Üzerine Bir İnceleme“, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 66: 57-63. https://doi.org/10.18070/erciyesiibd.1321823

Mollaoğulları, B., Öncü, S. (2020), “Denetim Komitesinin İç Denetim Birimi Çalışmalarına Etkisi: Türkiye’de İç Denetim Birimi Yöneticilerinin Algısı Araştırması”, Yönetim ve Ekonomi Dergisi, 27: 405-424.

Muneeza, İ.A., Wajeeh, A, (2012), “Strategic Corporate Governance For Sustainable Mutual Development”, International Journal of Law and Management, 54/3:197-208.

Öksüz, F. (2014), “Hedeflerimize Ulaşmak İçin Riskleri Çok İyi Yönetmemiz Gerekiyor”, Iç Denetim Dergisi, 40: 67-82.

Öner, S., & Adiloğlu, B. (2019),“İşletmelerde Kurumsal Risk Yönetimi ve İç Denetime Farklı Bir Bakış Açısı 5S Uygulaması“, Muhasebe Enstitüsü Dergisi, 61: 67-82.

Özbilger, H. İ. (2021), “İç Denetime Yeni Bir Bakış: Üçlü Hat Modelinin Değerlendirilmesi“, Denetişim Dergisi 22: 40-54.

Özbilgin, G. (2012), “Risk ve Risk Çeşitleri”, Bilişim Dergisi, 145:86-93.

Özer, M. A., & Erdem, E. (2022), “Kurumsal Risk Yönetimi: Sorumlular ve Başarı Kriterleri Üzerinden Bir Değerlendirme“, Denetişim Dergisi, 25: 58-76.

Özsoy, M. T. (2012),”Yeni Türk Ticaret Kanunu ve Şirketlerde Kurumsal Risk Yönetimi, Mali Çözüm Dergisi, 110: 165-185.

Özyiğit, H., & Yıldırım, S. (2022),“Kurumsal Risk Yönetim Sisteminde Bağımsız Denetime Hazırlanma Süreci“, Muhasebe Bilim Dünyası Dergisi, 24/2: 365-391. https://doi.org/10.31460/mbdd.915334

Pierce, E. M., & Goldstein, J. (2018), “ERM and Strategic Planning: A Change in Paradigm”, International Journal of Disclosure And Governance, 15:51-59.

Prewett, K., & Terry, A. (2018),”COSO’s Updated Enterprise Risk Management Framework—A Quest For Depth And Clarity”, Journal of Corporate Accounting & Finance, 29/3: 16-23.

Ramamoorti, S. (2003d), ‘’Internal Auditing: History, Evolution, and Prospects’: .1-24. (https://na.theiia.org)

Radu, M. (2012), “Corporate Governance, Internal Audit and Environmental Audit - The Performance Tools in Romanian Companies”, Accounting and Management Information Systems, 11/1: 112–130.

Sarıtaş, H. & Kaya, Y. (2017),“KOBİ’ler İçin Kurumsal Risk Yönetimi ve Firmaların Risk Yönetimi Farkındalığı Üzerine Bir Araştırma“, Social Sciences, 12/4: 212-231.

Sha, H., Arkam, M., Hussain, M., Imran, S. & Rehman, K. U, (2011), “Relationship between risk perception and employee investment behavior”, Journal of Economics and Behavioral Studies, 6: 348.

Spears J. L. ve Barkı, H., (2010), “User Participation in Information Systems Security Risk Management”, MIS Quarterly, 34: 503-522.

Şahin, A.(2016), “Riskin Erken Teşhis Komitesi (TTK Md.378 ve 625/1-e’nin Değerlendirilmesi)”, İnönü Üniversitesi Hukuk Fakültesi Dergisi, 7/2: 287-314.

Thomas, M. (2007), ‘’The Seven-Step Process to Risk-Based Auditing’’, FSA Times: 1-6.

Töre, İ. (2021), “Kurumsal Yönetim Açısından Riskin Erken Saptanması ve Yönetimi Komitesi, Eksiklikleri ve Çözüm Önerileri”, Optimum Ekonomi ve Yönetim Bilimleri Dergisi, 8/1:145-164.

Tüm, K. (2015), “Muhasebe Hilelerinin Önlenmesinde İç Kontrol Sisteminin Önemi Üzerine Bir Araştırma”, Giresun İİBF Dergisi, 1/1:105-128.

Türedi, H. Karakaya, G., İldem, M.(2015), “Kurumsal Yönetim ve İç Denetim İlişkisi”, Sayıştay Dergisi. 96: 55-74.

Türedi, H., Zor, Ü., & Gürbüz, F. (2015),“Risk Odaklı İç Denetim“, Muhasebe Ve Finansman Dergisi, 66: 1-20. https://doi.org/10.25095/mufad.396528

Tranchard, S. (2018), “The New ISO 31000 Keeps Risk Management Simple”, Cenova: ISO.

Usman, Ö. (2020),” Kurumsal Risk Yönetim Sisteminin İşletmelere Getirdiği Yenilikler ve Geleneksel Risk Yönetim Sistemi ile Karşılaştırılması“, Turkish Studies - Economy,15/4: 2509-2528.

Usman, Ö. (2018),“Kurumsal Risk Yönetim Sisteminde Risk Değerlendirme Raporlarının Hazırlanması“, Uluslararası Toplum Araştırmaları Dergisi, 9/16: 1588-1612.

Usman, Ö.& Kaygusuz, S. Y. (2019),“Kurumsal Risk Yönetiminde Uygulanması Gereken Adımlar. Muhasebe ve Denetime Bakış”, 18/56: 109-128.

Uysal, M. (2018), “ISO 31000 ve COSO Kurumsal Risk Yönetimi Karşılaştırması: Çerçeveleri Anlamak“, Denetişim Dergisi, 22: 55-68.

Uysal, M. (2020),“Stratejik Risklerin Yönetilmesi ve Örgütlerde Sürekli Risk Yönetimi Entegrasyonu“, Denetişim Dergisi, 21: 39-52.

Uzunoğlu, E. & Öksüz, B. (2013),“Kurumsal İtibar Riski Yönetimi: Halkla İlişkilerin Rolü“, Selçuk İletişim, 5/3: 111-123. https://doi.org/10.18094/si.44795

Vasile, E. & Simion, D. O. (2019). “The Role of Information Systems in Economic Organizations for The Strategic Management”, Internal Auditing & Risk Management, 14/2: 9-24.

Yereli, A. N. (2007), “Muhasebe Bilgi Sistemlerinin Risk Yönetimine Yönelik Bir Araştırma”, Muhasebe Ve Denetime Bakış Dergisi, 23: 15-32.

DİĞER KAYNAKLAR

Bailey, J.A., (2010), The IIA’s Global Internal Audit Survey: A Component of the CBOK Study, Core Competencies for Today’s Internal Auditor (Günümüz İç Denetçilerinin Temel Yetkililikleri), Report II, The Institute of Internal Auditor Research Foundation, Florida, 978-0-89413-697-9

Borucu,A., (2019), Kurumsal Risk Yönetimi Projelerinde Risk Değerleme Sürecinin İşlevi, www.denetimnet.com

Burca, N.(2017), Yenilenen COSO Kurumsal Risk Yönetimi Çerçevesi, https://nazifburca.com/2017.09.20/yenilenen-coso-kurumsal-risk-yonetimi-cercevesi/

Burca, N.(2024), Yeni Global İç Denetim Standartlarıyla Yapılan Önemli Değişiklikler, https://nazifburca.com/2024/01/11/yeni-global-ic-denetim-standartlariyla-yapilan-onemli-degisiklikler/

Carmichael, M., (2022), “Risk Appetite vs. Risk Tolerance: What is the Difference? https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/risk-appetite-vs-risk-tolerance-what-is-the-difference?gad_source=1&gclid=CjwKCAjw7NmzBhBLEiwAxrHQ-bD_WJ_cZeGnQkKO5FRGuzkhdYWkccrjoplLNe-1Zt3M9VhFSok-yRoC5ckQAvD_BwE

COSO, (2004), Enterprise Risk Management Framework, https://www.coso.org/guidance-erm

COSO (2013), Enterprise Risk Management Framework, https://www.coso.org/guidance-erm

COSO (2017), Enterprise Risk Management Executive Summary, https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Çevikbaş, Rafet, Türkiye'de İç denetim Kurumu, Türk İdare Dergisi • Sayı: 471-472 • Haziran - Eylül 2011

Deloitte, (2019), Global Risk Management Survey.

Deloitte, (2020), "G20 OECD Kurumsal Yönetim İlkeleri Üzerine…" , G20 OECD Kurumsal Yönetim İlkeleri Üzerine.pdf (deloitte.com)

Emhan, A, (2006), "Risk Yönetiminden Ne Anlıyoruz? Birliğimizdeki Uygulama Durumu Nedir?", 7 nci Ana Jet K.lığı Üs Uçuş ve Yer Emniyeti Semineri.

Hazine ve Maliye Bakanlığı Yayınları, (2019), Kurumsal Risk Yönetimi Bütüleşik Çerçeve-COSO. https://ms.hmb.gov.tr/uploads/2019/01/Kurumsal-Risk-Y%C3%B6netimi-B%C3%BCt%C3%BCnle%C5%9Fik-%C3%87er%C3%A7eve-COSO.pdf

Kurumsal Yönetim İlkelerinin Belirlenmesine ve Uygulanmasına İlişkin Tebliğ, 30.12.2011, 28158 nolu Resmi Gazete.

The Institute of Internal Auditors, (2013). IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control.

The Institute of Internal Auditors, (2010). Uluslararası İç Denetim Standartları.

The Institute of Internal Auditors, (2017). Uluslararası İç Denetim Standartları.

İlker Açıkalın, (2012). Kurumsal Risk Yönetimi, KPMG, İstanbul.

IIA, (2024), "Global Internal Audit Standards".globalinternalauditstandards_2024january9_printable.pdf (theiia.org)

Internal Control–Revised Guidance for Directors on the Combined Code, (2005), Financial Reporting Council. .https://www.accountancyeurope.eu/wp content/uploads/FRC_Revised_Guidance_for_Directors_on_Combined_Code_051027102005121030.pdf

https://strateji.iyte.edu.tr/wp-content/uploads/sites/108/2019/10/INTOSAI-%C4%B0%C3%A7-Kontrol-Standartlar%C4%B1-K%C4%B1lavuzu.pdf

IPPF, (2019), “Assessing The Risk Management Process”. https://iia-p.org/wp-content/uploads/2020/02/IPPF-PG-Assessing-the-Risk-Management-Process.pdf.

İstanbul Serbest Muhasebeci ve Mali Müşavirler Odası. (2015, Nisan), İç denetime genel bir bakış

ISO 31000 Risk Management (2018)
https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf

ISO 31000 Risk Management A Practical Guide (2021)
https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100464_preview.pdf

INTOSAI Development Initiative, (2018), Compliance Audit Issaı Implementation Handbook, INTOSAI Development Initiative.

IRM, Institute of Risk Management,. (2012), Risk Culture: Resources for Practitioners. London.

Knight, F.H.(1921) “Risk, Uncertainty and Profit”, Hart, Houghton Mifflin.

Kamu Gözetim Kurumu (2017), İstanbul Muhasebe ve Denetim Sempozyumu, Ankara, Önka Basım Yayın.

Lancaster, A., Goff, S, (2023), Financial Risk Management Fundamentals. https://www.auditboard.com/blog/financial-risk-management/

Locklear, K. (2012), ”Toward a Theory of Everything? Exploring at the Edges of the ERM Construct, Enterprise Risk Management Symposium.

Madendere, M. A, (2005), “Kurumsal Risk Yönetiminde İç Denetim Rolü, (Çeviri/Derleme)”, TİDE.

Mattie, J.A. ve D.L. Cassidy. (2008), “Achieving Goals, Protecting Reputation: Enterprise Risk Management for Educational Institutions”. http://www. universityofcalifornia.edu/regents/regmeet/july08/a7a.pdf.

OECD, 2023, G20/OECD Principles of Governance.

OECD, 2015, G20/OECD Kurumsal Yönetim İlkeleri,

https://www.oecd.org/daf/ca/Corporate-Governance-Principles-TUR.pdf

PwC, (2023), Global Risk Survey.

PWC, (2017), “How and When Should You Leverage Internal Audit”.

https://assets.hcca
info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2017/508print2.pdf

Saka, T. (2008), “Kurumsal Risk Yönetimi ve 2008 Yılı Risk Öngörüleri”, TÜSİAD, tusiad.org/tr/tum/item/download/2468_47d48b480878ef141e0ded0518703d78.

Saka, T., Uğural, A. (2008), “Kurumsal Risk Yönetimi Nedir?” Semineri, TÜSİAD. https://tusiad.org/tr/tum/item/2622-kurumsal-risk-yonetimi-nedir-semineri

Schmidt, M. (2004). Investigating risk perception: A short introduction, Austria, 3. Web: http://faculty.mercer. edu/butler_aj/documents/Intro_risk_perception_ Schmidt.pdf.

Tekgül, E. (2007, Kasım), “Kurumsal Risk Yönetimi ve Risk Zekası”, Referans Gazetesi.

Tekin, S. (2020) “Risk Toplumu ve Toplumsal Tecrit”, Birikim Dergisi, https://birikimdergisi.com/guncel/10045/kuresel-risk-toplumu-ve-toplumsal-tecrit.

Türkiye Kurumsal Yönetim Derneği (TKYD), (2004), Kurumsal Yönetim Derneği “Ekonomik İşbirliği Ve Kalkınma Örgütü Kurumsal Yönetim İlkeleri”

https://www.tkyd.org/wp-content/uploads/2022/12/oecd2004.pdf

Türkiye Kurumsal Yönetim Derneği (TKYD), 2023, Cumhuriyet’in 100.Yılında Kurumsal Yönetimin 20 Yılı.TKYD-20-YIL-KITABI.pdf

TÜSİAD, “Kurumsal Yönetim En İyi Uygulama Kodu: Yönetim Kurulunun Yapısı ve İşleyişi”, Yayın No: 336, İstanbul, Aralık 2002.

TÜSİAD (2006) , Kurumsal Risk Yönetimi (Risk ve Değer Yönetimi Çalışma Grubu), Ankara.

TİDE (2008), Uluslararası İç Denetim Standartları, Kırmızı Kitap, İstanbul.

TİDE (2017), Uluslararası İç Denetim Standartları, İstanbul.

TBB Çalışma Grubu, (2006), “Risk Yönetimi Prensipleri”, Bankacılar Dergisi, 57: 15-32. https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/riskyonetimi.pdf

TÜSİAD, (2008), Risk Yönetimi Çalışma Grubu, Kurumsal Risk Yönetimi, Yayın No. TÜSİAD-T/2008-02/452.

Türkiye İç Denetim Enstitüsü (2010), Uluslararası İç Denetim Standartları, Uluslararası Mesleki Uygulama Çerçevesi (UMUÇ), İstanbul.

Uzay, Ş. (2010), “Reel Sektörde İç Denetim Uygulamaları: Tespit ve Öneriler”, İstanbul, TÜSİAD Yayınları.

Van Der Erst, C., Van Daelen, M. (2009), “Risk Management in European and American Corporate Law”, ECGI Law Working Paper, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1399647.

World Economic Forum, (2024),The Global Risk Report.

Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ, Seri X, No:22, On dördüncü Kısım, İkinci Bölüm, Md.6.

Yurtseven, Gürdoğan, 2017 Teftişten İç Denetime Banka Müfettişliği, Beta Yayın evi,

EKLER

Ek-1

Bölüm-1

Demografik Sorular

1) Anketi dolduran kişinin unvanı
    a) Kurumsal Risk Yönetimi Yöneticisi/Kıdemli Uzmanı
    b) İç Denetim Yöneticisi/Kıdemli Uzmanı
    c) Riskin Erken Teşhisi Komitesi Üyesi
    d) Denetim Komitesi Üyesi
    e) Diğer (Lütfen Belirtiniz)
2) Anketi dolduran kişinin bu iş alanındaki toplam tecrübesi
    a) 0-5 yıl
    b) 5-10 yıl
    c) 10 yıl üzeri
3) Anketi dolduran kişinin sahip olduğu mesleki sertifikalar (Birden fazla belge var ise, çoklu seçim yapılabilir.)
    a) Uluslararasi İç Denetçi Sertifikası (CIA)
    b) Uluslararası risk yönetimi sertifikası (CRMA)
    c) Uluslararası hile denetçisi sertifikası (CFE)
    d) SMM/YMM
    e) Mevcut Değil
    f) Diğer (Lütfen belirtiniz)
4) İşletmenin faaliyet konusu nedir?
    a) Finansal Hizmetler
    b) Holding
    c) Üretim
    d) Satış/Pazarlama
    e) Diğer (Lütfen belirtiniz)

Bölüm 2

İç Denetimin Güvence Ve Danişmanlik Faaliyeti Kapsaminda Kurumsal Risk Yönetimi Sistemini Değerlendirme Sürecini Tespit Etmeye Yönelik Sorular

2.1.Kurumsal Risk Yönetimi Ve İç Denetim İle İlgili Genel Sorular

1) İşletmenizde aşağıdaki komitelerden hangileri mevcuttur? (Birden fazla seçenek işaretleyebilirsiniz.)
    a) Kurumsal risk yönetimi/riskin erken saptanması komitesi (Lütfen ankete devam edin.)
    b) Denetim komitesi (Lütfen 4.sorudan devam edin)

2) İşletmenizde riskin erken teşhisi komitesi, yönetim kuruluna bir yılda kaç kere rapor verir?
    a) 2'den az
    b) 2-4 arası
    c) 4-6 arası
    d) 6'nın üzeri
3) İşletmenizde riskin erken teşhisi komitesinin 1 yıl içinde gerçekleştirdiği toplantı sayısı kaçtır?
    a) 2'den az
    b) 2-4 arası
    c) 4'ün üzeri
4) İşletmenizde denetim komitesi, yönetim kuruluna bir yılda kaç kere rapor verir?
    a) 2'den az
    b) 2-4 arası
    c) 4-6 arası
    d) 6'nın üzeri
5) İşletmenizde denetim komitesinin 1 yıl içinde gerçekleştirdiği toplantı sayısı kaçtır?
    a) 2'den az
    b) 2-4 arası
    c) 4'ün üzeri
6) İşletmenizde kurumsal risk yönetimi birimi mevcut mudur?
    a) Evet, mevcuttur. (Lütfen ankete devam edin.)
    b) Hayır, mevcut değildir (Lütfen bu bölümde 9.soruya geçin.)
7) Kurumsal risk yönetimi birimi, hangi bölüme (fonksiyonel) raporlama yapmaktadır?
    a) Kurumsal risk yönetimi birimi doğrudan yönetim kuruluna bağlıdır.

b) Kurumsal risk yönetimi birimi, öncelikli olarak riskin erken saptanması/teşhisi komitesine bağlıdır.
c) Kurumsal risk yönetimi birimi, doğrudan Genel Müdür'e bağlıdır.
d) Diğer (Lütfen belirtiniz)

8) İşletmenizde kurumsal risk yönetimi birimi toplamda kaç çalışandan oluşmaktadır?
   a) 0-5 kişi
   b) 5-15 kişi
   c) 15 kişi üzeri

9) İşletmenizde iç denetim birimi mevcut mudur?
   a) Evet, mevcuttur. (Lütfen ankete devam edin.)
   b) Hayır, mevcut değildir (Lütfen bölüm 2.2'ye geçin.)

10) İç denetimi birimi, hangi bölüme (fonksiyonel) raporlama yapmaktadır?
   a) İç denetim birimi doğrudan yönetim kuruluna bağlıdır.
   b) İç denetim birimi, öncelikli olarak denetim komitesine bağlıdır.
   c) İç denetim birimi, doğrudan Genel Müdür'e bağlıdır.
   d) Diğer (Lütfen belirtiniz)

11) İşletmenizde iç denetim biriminiz mevcut ise, ilgili birim kaç çalışandan oluşmaktadır?
   a) 0-5 kişi
   b) 5-15 kişi
   c) 15 kişi üzeri

12) İç denetim birimi (Teftiş) aşağıdaki hangi koşullara uygun nitelikte faaliyetler yürütür? (Birden fazla seçenek seçilebilir.)
   a) Uluslararası iç denetim standartlarını referans alarak faaliyetlerini yürütür.
   b) İç denetim yönetmeliğinde iç denetim birimi çalışma usul ve esaslarını düzenleyen iç denetim standartlarına uygun çalışılacağı esası yer alır.
   c) İç denetim birimi, IIA'in uluslararası kalite güvence geliştirme programından geçmiştir. Raporlamalarda, denetimlerimiz uluslararası iç denetim standartlarına uygun şekilde yapılmıştır ibaresi kullanılmaktadır.

13) Iç denetim biriminde hangi sertifikalara sahip denetçiler vardır? (Birden çok seçenek işaretleyebilirsiniz.)
   a) Uluslararası iç denetçi sertifikası (CIA)
   b) Uluslararası hile denetçisi sertifikası (CFE)
   c) Uluslararası risk yönetimi sertifikası (CRMA)
   d) Bağımsız denetçi sertifikası (KGK)

e) Yeminli mali müşavir (YMM) ya da serbest muhasebeci mali müşavir (SMM)
f) Diğer (Lütfen belirtiniz)…

2.2. İç Denetimin Kurumsal Risk Yönetimi Olgunluk Düzeyini Belirlemesine Yönelik Sorular

1) İşletmenizde sürekli takip edilen bir kurumsal risk yönetimi süreci mevcut mu?
   a) Evet (Lütfen ankete devam edin.)
   b) Hayır ((Lütfen bölüm 2.3'e geçin.)
2) Aşağıda belirtilen kurumsal risk yönetimi sürecinin adımları işletmenizde uygulanıyor mu? (Birden çok seçenek işaretleyebilirsiniz.)
   a) Risk belirleme
   b) Risk önceliklendirme
   c) Risk değerlendirme
   d) Önlem planı yapma ve uygulama
   e) İzleme
   f) Raporlama
   g) Diğer (Lütfen belirtiniz)…
3) Temel aldığınız risk yönetimi modelini belirtir misiniz?
   a) COSO
   b) ISO 31000
   c) Diğer (Lütfen belirtiniz)…
4) İşletmenizde kurumsal risk yönetimi sürecini belirleyen ayrı bir yönetmelik (işletmenize özel) mevcut mudur?
   a) Evet
   b) Hayır
5) Kurumsal risk yönetimi süreci içinde sadece riskleri mi yoksa risklerle birlikte fırsatları da takip ediyor musunuz?
   a) Sadece riskler
   b) Riskler ve fırsatlar
6) Kurumsal risk yönetimi bakış açısı karar alma, hedef belirleme süreçlerine dahil edilmiş midir?
   a) Evet
   b) Hayır
7) İşletmenizde risk iştahı (Bir işletmenin kabul etmeye istekli olduğu risk düzeyi) belirlemesi yapılıyor mu?
   a) Evet (Lütfen ankete devam edin.)

b) Hayır (Lütfen bölüm 2.3.'e geçin.)

8) İşletmenizde risk iştahı belirleme hangi aralıklarla güncellenir?
   a) 6 ay-1 yıl
   b) 1-2 yıl
   c) 3 ve üzeri

9) Kurumsal risk yönetimi birimi, ilgili sürece yönelik olarak kontrol öz değerlendirme yaklaşımını uygular mı?
   c) Evet (Lütfen ankete devam edin.)
   d) Hayır (Lütfen bu bölümde 13.soruya geçin.)

10) Hangi öz değerlendirme yöntemlerini kullanır?
   a) Grup çalışması
   b) Anket çalışması
   c) Birebir görüşme
   d) Diğer (Lütfen belirtiniz)

11) İç denetim, denetim hizmeti süresince kontrol öz değerlendirme çalışmalarının sonuçlarını kullanır mı?
   a) Evet
   b) Hayır

12) İç denetçiler, KRY denetiminde kontrol öz değerlendirme yaklaşımını genelde hangi amaçlar için kullanır?
   a) Finansal risklerin denetimi
   b) Mevzuat-uygunluk risklerinin denetimi
   c) Operasyonel risklerin denetimi
   d) Diğer (Lütfen belirtiniz)

13) Üst yönetim, kurumsal risk yönetimi sürecinin etkililiğini hangi yöntemlerle takip eder? (Birden fazla seçenek işaretleyebilirsiniz.)
   a. İşletmede mevcut olan risk yönetimi el kitabı/prosedürüne göre inceler.
   b. Kurumsal risk yönetimi ekibinin kontrol öz değerlendirme kapsamındaki tespitlerini dinler.
   c. İç denetim raporlarında yer alan bulguları takip eder.
   d. İç denetim/kurumsal risk yönetimi amacıyla kullanılan yazılımlar aracılığıyla takip eder.
   e. Diğer (Lütfen Belirtiniz)

2.3. İç Denetimin Verdiği Hizmetin Niteliğini Ölçmeye Yönelik Sorular

1) İç denetim biriminin yıllık planlarında kurumsal risk yönetimi denetimi var mıdır?
    a) Evet
    b) Hayır
2) Şimdiye kadar kurumsal risk yönetimi sürecine yönelik bir iç denetimden geçtiniz mi?
    a) Evet (Lütfen ankete devam edin.)
    b) Hayır(Lütfen bu bölümde 5.soruya geçin.)
3) İç denetim sonucunda iç denetçi sürece yönelik nasıl tespitlerde bulundu?
    a) İç denetçi, sadece sürecin yürütülme şekline, süreçteki eksik ve sıkıntılara yönelik tespitte bulundu.
    b) İç denetçi, sadece sürece yönelik iyileştirme önerilerinde bulundu.
    c) İç denetçi hem sürecin yürütülmesindeki eksikleri, sıkıntıları hem de iyileştirme önerilerinde bulundu.
4) İşletmenizde kurumsal risk yönetimi sürecine yönelik iç denetim aşağıdaki hizmetlerden hangisini/hangilerini verir?
    a) Güvence hizmeti
    b) Danışmanlık hizmeti
    c) İkisi de
5) Son 2 yıl içinde KRY'ye yönelik saptanan politikalara uyulmadığına ilişkin herhangi bir tespit yapılmış mıdır?
    a) Evet
    b) Hayır
6) İç denetim birimi, kurumsal risk yönetimi denetiminde aşağıdaki rollerden hangilerini üstlenir? (Çoklu seçim yapmanızı rica ederiz.)
    a) Risk yönetimi sürecinde güvence vermesi
    b) Risklerin doğru değerlendirildiğine dair güvence vermesi
    c) Risklere yönelik alınan aksiyonların uygulandığına dair güvence vermesi
    d) Risk yönetimi sürecinin değerlendirilmesi
    e) Temel risklerin yönetimi ve raporlanmasının değerlendirilmesi
    f) Risklerin tanımlanmasını ve değerlendirilmesini gözden geçirme
    g) Risklere cevap vermede işletmeye koçluk yapma
    h) KRY faaliyetlerini koordine etme
    i) KRY süreci sonunda risk haritasının çıkarılmasını sağlama
    j) KRY sürecinin iyileştirilmesi
    k) KRY sürecinin işletmede kurulumunun desteklenmesi

l) Yönetim kurulu onayı için risk yönetimi stratejisi geliştirme
m) Risk iştahını ayarlama
n) Risk yönetimi süreçlerini doğrudan uygulama
o) Risk yanıtları konusunda karar alma
p) Risk yönetimi için hesap verilebilirliğin sağlanması

7) İç denetim bölümü, kurumsal risk yönetimi sürecine yönelik hazırlanan iç denetim raporunu hangi birime sunulmaktadır?
   a) Denetim komitesi
   b) Kurumsal risk yönetimi/riskin erken teşhisi komitesi
   c) Doğrudan Genel Müdür'e
   d) Hepsi
8) Kurumsal risk yönetimine yönelik iç denetim yapılırken iç denetçiler ve risk yöneticileri arasında çatışma olur mu?
   a) Evet (Lütfen ankete devam edin.)
   b) Hayır (Lütfen bölüm 2.4'e geçin.)
9) İç denetim esnasında iç denetçiler ve kurumsal risk yönetimi birimi arasında çatışma olduğunda, bu sorunu nasıl çözüyorsunuz? (Kısaca yazabilir misiniz?)

2.4. İç Denetim Sürecinin Etkililiğini Ölçmeye Yönelik Sorular

1) İşletmenizdeki iç denetim birimi, çalışmaları esnasında organizasyonda bağlı olduğu kurul/kişiden bağımsız ve tarafsız hareket edebilmekte midir?
   a) Tamamen bağımsızdır
   b) Genelde bağımsız olsa bile bazen müdahaleler olmaktadır.
   c) Bağımsız değildir.
2) İç denetim raporundaki tavsiyeler ve alınması gereken aksiyonlar, işletme tarafından gerçekleştiriliyor mu?
   a) Evet, titizlikle gerçekleştiriliyor.
   b) Kısmen gerçekleştiriliyor.
   c) Hayır, gerçekleştirilmiyor.
3) İç denetim bulgularının takibi, yine iç denetim birimi tarafından düzenli yapılıyor mu?
   a) Evet (Lütfen ankete devam edin.)
   b) Hayır (Lütfen bu bölümde 5.soruya geçin)
4) İç denetim birimi, iç denetim bulgularının takibini ne sıklıkla yapar?

a) 0-3 aylık dönemlerde
b) 4-6 aylık dönemlerde
c) 7-12 aylık dönemlerde
d) Yıllık

5) Yönetim kurulu/üst düzey yöneticiler ne sıklıkla iç denetim raporunda yer alan bulgulara yönelik gelişmeleri takip ederler?
   a) 0-3 aylık dönemlerde
   b) 4-6 aylık dönemlerde
   c) 7-12 aylık dönemlerde
   d) Düzensiz takip mevcut
   e) Takip mevcut değil
6) İç denetim bulgularının işletmenizde ele alınış şeklini nasıl tarif edersiniz?
   a) Bulgular ehemmiyetle değerlendirilir ve tüm bulgular ile ilgili aksiyon alınır.
   b) Bulgular değerlendirilir ve sadece kritik bulgular ile ilgili aksiyon alınır.
   c) Bulgular belli dönemlerde takip edilir.
   d) Bulgular takip edilmez.
7) İç denetimin etkililiğini ölçüyor musunuz?
   a) Evet (Lütfen ankete devam edin.)
   b) Hayır (Anket tamamlanmıştır.)
8) İç denetimin etkililiğini ölçerken aşağıdaki noktalardan hangilerini dikkate alırsınız? (Birden çok seçenek seçebilirsiniz.)
   a) İç denetim planına uygun zamanda iç denetimin tamamlanması
   b) İç denetim raporunun ne kadar sürede hazırlandığı
   c) İç denetim bulgularının iç denetçiler tarafından düzenli takip edilip edilmemesi
   d) Diğer (Lütfen belirtiniz)

Ek-2

BIST 50 ŞİRKETLERİ	
AKBANK	KONTROLMATİK TEKNOLOJİ
ALARKO HOLDİNG	KOZA ANADOLU METAL
ALFA SOLAR ENERJİ	MİA TEKNOLOJİ
ARÇELİK	MİGROS
ASELSAN	ODAŞ ELEKTRİK
ASTOR ENERJİ	OYAK ÇİMENTO
BİM	PEGASUS
BORUSAN BİRLEŞİK BORU	PETKİM
CW ENERJİ	SASA
ÇİMSA ÇİMENTO	SMART GÜNEŞ ENERJİSİ
DOĞAN HOLDİNG	TAV HAVALİMANLARI
DOĞUŞ OTOMOTİV	TOFAŞ
EGE ENDÜSTRİ	TURKCELL
EMLAK KONUT	TÜPRAŞ
ENERJİSA	THY
ENKA	TÜRK TELEKOM
EREĞLİ DEMİR ÇELİK	GARANTİ BANKASI
EURO POWER ENERJİ	HALK BANKASI
FORD OTOMOTİV	İŞ BANKASI
GİRİŞİM ELEKTRİK SANAYİ	ŞİŞECAM
GÜBRE FABRİKALARI	ÜLKER
HACI ÖMER SABANCI HOLDİNG	VAKIFBANK
HEKTAŞ	VESTEL
KARDEMİR	YAPI KREDİ BANKASI
KOÇ HOLDİNG	ZORLU ENERJİ